TRABAJO DE GRADO

ANÁLISIS DE LA IMPLEMENTACIÓN DE LISTAS DE CONTROL DE ACCESO (ACL), PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA CRAWFORD COLOMBIA LTDA

BELISARIO ANTONIO GARCIA MARTINEZ
HENRY ARTURO MORENO DUARTE

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2021

TRABAJO DE GRADO

ANÁLISIS DE LA IMPLEMENTACIÓN DE LISTAS DE CONTROL DE ACCESO (ACL), PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA CRAWFORD COLOMBIA LTDA

BELISARIO ANTONIO GARCIA MARTINEZ
HENRY ARTURO MORENO DUARTE

Docente

INGENIERO: CARLOS MAURICIO BLANCO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2021

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

1. INTRODUCCIÓN

A medida que se incremente el uso de las transacciones y actividades empresariales a través del internet, las aplicaciones y los servicios basados en las redes incorporan mayores riesgos a la confidencialidad, integridad y disponibilidad de la información de los individuos y de las empresas. En algunas ocasiones la seguridad de la red se puede ver comprometida y la información que es de suma importancia, sin la protección adecuada, puede estar en riesgo de confidencialidad.

Debido a la creciente demanda de computadoras para el uso doméstico y comercial, estas son el objeto de ataques constantes de una variedad de amenazas en continua evolución que afectan al rendimiento, las comunicaciones y la confiabilidad de las mismas. *"Es por esto que actualmente la seguridad de la información ha cobrado importancia en las redes de datos, dando como resultado el surgimiento de una gran variedad de topologías en las cuales el objetivo principal es mitigar los posibles ataques que permitan el robo o alteración de la información al interior de las redes."* [1]

Gracias a esto se ha logrado determinar que, uno de los grandes retos a los que se enfrentan hoy en día los sistemas de información, gracias a la gran acogida que tiene la tecnología y los servicios basados en las redes, es como lograr resguardar los activos de información, ya que se puede afirmar que este activo representa gran importancia en cualquier negocio o empresa.

En la empresa CRAWFORD COLOMBIA LTDA y en la cual se adelantó la presente investigación, se logra evidenciar que, los routers soportan una gran variedad de servicios de red que permiten a los usuarios conectarse a la misma, algunos de estos servicios pueden restringirse o desactivarse, lo que mejora la seguridad sin que la operación de la red se vea afectada.

Teniendo en cuenta lo mencionado anteriormente, se analizan los requerimientos básicos con los que se deben contar para realizar la implementación de listas de control de acceso (ACL), haciendo énfasis en los roles y el principio del mínimo privilegio (PoLP), de acuerdo con los niveles de acceso que requiera cada colaborador de la empresa CRAWFORD COLOMBIA LTDA., para cumplir de manera óptima sus actividades diarias.

[1] Rincón Álvarez, Wiliam Alexander. Administración de políticas de seguridad en una red de datos bajo una estructura de red definida a través de la utilización del servidor pfense [En línea]. Bogotá: Universidad Santo Tomás, 2017., 13 p. disponible en http://repository.usta.edu.co/handle/11634/714

2. GENERALIDADES

1. LÍNEA DE INVESTIGACIÓN

La línea de investigación sobre la cual se enfoca el desarrollo del presente proyecto es Software Inteligente y Convergencia Tecnológica, ya que al realizar el análisis de la implementación de listas de control de acceso (ACL), permite determinar la optimización del tráfico de datos y seguridad de la información, en la empresa CRAWFORD COLOMBIA LTDA.

2. PLANTEAMIENTO DEL PROBLEMA

La seguridad de los sistemas informáticos, se ha tornado en un problema crítico en la mayoría de las empresas, debido a que algunos de los ataques se originan al interior de las mismas, es decir, por parte del usuario interno, convirtiéndose en uno de los vectores de ataque predilectos por los ciberdelincuentes, mediante el uso de la ingeniería social cual busca la explotación de las debilidades propias de los usuarios, lo cual hace necesario que las empresas realicen la implementación de estrategias enfocadas en la seguridad de la información, procurando realizar las evaluaciones pertinentes que permitan determinar las necesidades específicas de su negocio.

Teniendo en cuenta que CRAWFORD COLOMBIA LTDA, es una compañía ajustadora de seguros cuyo negocio principal es realizar el peritaje de siniestros que afectan pólizas de seguros, en donde en la mayoría de los casos la información suministrada por la aseguradora y el asegurado de un siniestro contiene documentación financiera y legal, toda esta documentación suministrada por los actores anteriormente mencionados es estrictamente confidencial ya que muestra en gran medida los procesos y procedimientos tanto de CRAWFORD COLOMBIA LTDA como de los clientes o Aseguradoras, por lo que cualquier tipo de filtración de información afectaría la imagen de la compañía de forma negativa causando falta de credibilidad por parte de sus clientes al grado de perder su nicho de trabajo.

De acuerdo a lo anterior, se hace pertinente verificar el estudio realizado por la Organización de Estados Americanos, titulado Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe, ya que en este estudio se logra evidenciar que los eventos de riesgo en la seguridad de la información más frecuentes contra los usuarios de servicios financieros son el phishing, la ingeniería social, y el software espía (malware o troyanos), los cuales también se pueden ver replicados en las ajustadoras de seguros y en cualquier otro entorno económico, en este estudio se hace énfasis en que, *"el 92% de las entidades bancarias manifiestan que identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital en contra de la entidad financiera. Los eventos más identificados fueron: i) el código malicioso o malware (80% del total de entidades bancarias), ii) la violación de políticas de escritorio limpio (clear desk) (63% del total de entidades bancarias), y, iii) el phishing dirigido para tener acceso a sistemas del banco."* [2] De acuerdo

[2] Pincay Gordillo, Óscar Eduardo. Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe [En línea]. Bogotá: Organización de Estados Americanos, 2018., 7 p. disponible en

a los datos que arrojan este tipo de estudios, se puede apoyar la toma de decisiones y la validación de estrategias a seguir, ya que refleja una realidad que está afectando al sector bancario, pero como se indicó anteriormente estos eventos se pueden ver replicados cualquier otro entorno económico.

A la par del incremento de eventos de riesgo en la seguridad de la información, es necesario estudiar las medidas que permitan robustecer la seguridad de la información, como lo es realizar el filtrado de los paquetes que se transmiten a través de las redes, para lograr controlar el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el bloqueo de estos según criterios determinados, lo anterior es expuesto en el libro titulado Seguridad Informática para Empresas y Particulares, donde se indica que: *"Los sistemas para el cifrado de datos en tránsito, los sistemas de detección de intrusiones (IDS) y las listas ACL para control de accesos al sistema de archivos están rondando un despliegue en torno al 75%,"*[3] la publicación de este tipo de estudios permite visualizar un futuro prometedor para la seguridad informática.

Adicionalmente es recomendable que, los roles y privilegios otorgados a los usuarios de los servicios de red, se basen en principios básicos de seguridad, como el principio del mínimo privilegio (PoLP), esto para procurar brindar los permisos necesarios que requiera cada colaborador de las empresas para cumplir de manera óptima sus actividades diarias, sin afectar el correcto funcionamiento de las redes, teniendo en cuenta que las bases de este principio son la reducción de la superficie expuesta a ciberataques, la detención de la propagación del malware, la mejora de la productividad del usuario final y la ayuda a agilizar el cumplimiento y las auditorías, lo anterior es explicado en el portal web de la empresa de software Cyberark, donde se indica que: *"en general, el principio del mínimo privilegio se considera una práctica óptima de ciberseguridad y es un paso fundamental para proteger el acceso con privilegios a datos y activos de gran valor."*[4]

De acuerdo con lo expuesto anteriormente, a la observación y seguimiento realizado a la empresa CRAWFORD COLOMBIA LTDA, y teniendo en cuenta que la empresa puede llegar a ser víctima de eventos de riesgo en la seguridad de la información, se pretende determinar que política ACL, se ajusta mejor a las políticas de seguridad de la información existentes, infraestructura y necesidades específicas del negocio, teniendo en cuenta que la empresa no cuenta con restricciones en el tráfico de red, la implementación de listas de control de acceso (ACL), pueden restringir o desactivar algunos servicios sin que la operación de la red se vea afectada, adicionalmente se logra evidenciar que los usuarios no cuentan con restricciones de acceso a los recursos de red, lo cual, puede comprometer la seguridad de los activos de la información y afectar la óptima operación de la red de la empresa, todo esto con el objetivo de lograr fortalecer la integridad, disponibilidad y confidencialidad de la información, y así poder proteger y asegurar, de una mejor manera, estos activos.

https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf informacion_20200526.html

[3] Álvarez Marañón, Gonzalo y Pérez García, Pedro Pablo. Seguridad informática para empresas y particulares [En línea]. Madrid: Editorial McGraw Hill, 2004, 50 p. disponible en https://online.fliphtml5.com/oazu/cgdk/#p=50

[4] Cyberark. Principio del Mínimo Privilegio (PoLP) [En línea]. Bogotá: Cyberark, s.f., disponible en https://www.cyberark.com/es/what-is/least-privilege/

2.2.1. ANTECEDENTES DEL PROBLEMA

Durante los últimos años se han venido desarrollando diversas investigaciones en el área de la seguridad de la información, con el fin de reducir los riesgos a los que se enfrentan las empresas en el tratamiento de los activos de la información, a continuación, se relacionan documentos existentes que explican temáticas relacionadas y que ayudan a reafirmar la importancia de la seguridad de la información:

De acuerdo con la guía práctica para implementar la seguridad de la información publicada por la compañía Globaltek Security, titulada Inseguridad de la información, es importante resaltar que las: *"encuestas de la XIII jornada internacional de seguridad informática en Colombia/2013, www.acis.org.co, concluyen que en Colombia la norma ISO 27001 es el estándar más usado en la realidad nacional con un 62.35% de participación, ITIL con un 37% de participación y Cobit en tercer lugar con el 31% de selección por parte de los encuestados"*[5], de acuerdo con el Ingeniero Andres Almanza, quien en su momento adelanto la mencionada encuesta, se debía realizar reflexión, ya que en el año 2013 existía un porcentaje (26.54%) que no consideraba relevante seguir un protocolo o norma de seguridad de la información.

Figura 1. *Sistemas de gestión de seguridad de la información más usados en Colombia*

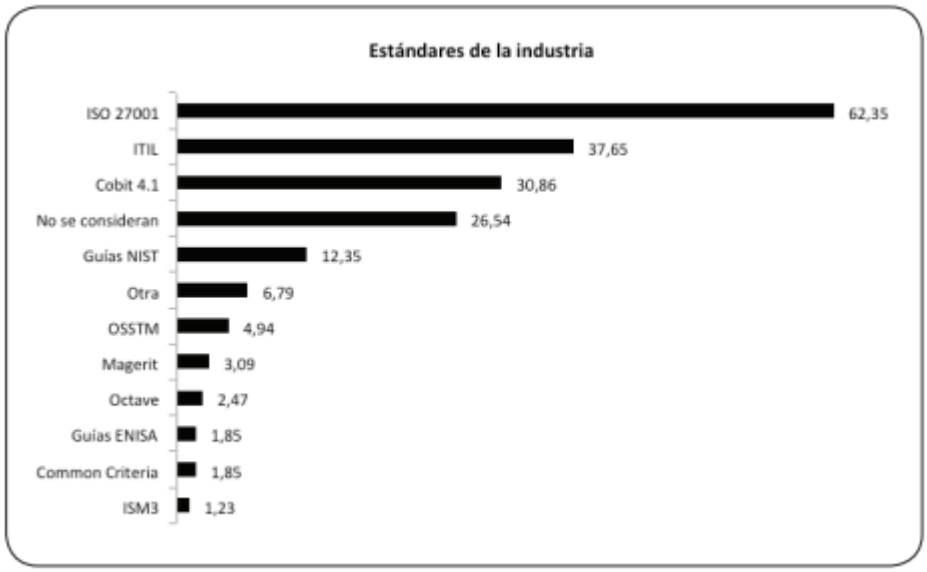

Figura 1. Sistemas de gestión de seguridad de la información más usados en Colombia

Fuente: Guía Práctica Para Implementar La Seguridad De La Información (Carvajal, 2013)

Tomando como punto de partida la guía práctica citada anteriormente, se puede realizar una comparación frente el estudio titulado Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018 publicado por la Revista Ibérica de Sistemas e

[5] Carvajal, Armando. INSEGURIDAD DE LA INFORMACIÓN [En línea]. Bogotá: Globaltek, 2013., 19 p. disponible en https://www.globalteksecurity.com/docs/book/INSEGURIDAD_DE_LA_INFORMACION.pdf

Tecnologias de Informação en su edición N.º E27, 03/2020, en el cual se realizó un estudio a la evolución de la Seguridad de la Información en Colombia, en sectores económicos como la educación 16%, los servicios financieros 15%, gobierno 14%, y la consultoría especializada 13%, ya que son estos sectores los que han participado consistentemente durante los últimos 18 años. Las encuestas realizadas arrojaron los siguientes datos, *"Los Virus/Caballos de troya a lo largo de este estudio se han mostrado como la presencia más significativa con un 42%; sin embargo, no es el que más crece en el tiempo. Las instalaciones de software no autorizado 28%, Ingeniería social 26%, Phishing 23% y Ransomware 18%, son los de crecimiento sostenido durante los años."*[6]

Cabe resaltar que, para lograr concientizar a las empresas, de los sectores mencionados, en los temas referentes a seguridad de la información, la Asociación Colombiana de Ingenieros de Sistemas (ACIS) ha venido realizando grandes esfuerzos, por más de 19 años a la fecha de publicación del estudio en mención, aplicando una serie de encuestas de seguridad de la información con el fin de estudiar y entender el comportamiento de la seguridad en el contexto colombiano, dichas encuestas han arrojado resultados relevantes en materia de seguridad de la información, una de estas encuestas realizadas muestra una tendencia al alza en la dependencia a las áreas de seguridad de la información al interior de las empresas colombianas.

Figura 2. *Dependencia del área de seguridad de la información*

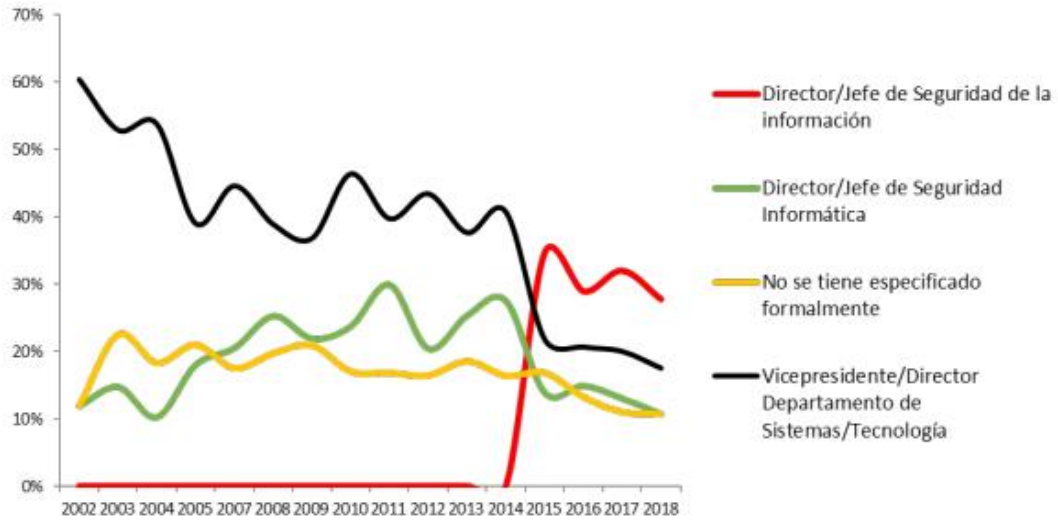

Figura 2. Dependencia del área de seguridad

Fuente: Revista Ibérica de Sistemas e Tecnologias de Informação (Cano M. & Almanza, 2020)

[6] Cano M, Jeimy J y Almanza, Andres. Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018 [En línea]. Bogotá: Revista Ibérica de Sistemas e Tecnologias de Informação, 2020., 477 p. disponible en https://www.researchgate.net/project/Encuesta-Colombiana-de-Seguridad-Informatica

Una vez realizada la consolidación de 18 años de recolección de información mediante encuestas enfocadas en describir la realidad de la seguridad de la información en Colombia, realizadas por la Asociación Colombiana de Ingenieros de Sistemas (ACIS), *"se pueden observar que los sectores como el Financiero, el sector Gobierno, la Educación, Consultoría Especializada y las Telecomunicaciones, han sido los que muestran más entusiasmo por entender sus dinámicas en materia de seguridad y control. Se espera que siga creciendo la participación de estos sectores en la realización del ejercicio en los años futuros."*[7]

El observatorio tecnológico del ministerio de educación, cultura y deporte del gobierno de España, publicó el monográfico titulado, listas de control de acceso (ACL), donde indican que, las ACL listan mediante una serie de condiciones establecidas, que tipo de tráfico puede viajar por la red en dirección a la interfaz del router, *"Las ACL indican al router qué tipo de paquetes aceptar o rechazar en base a las condiciones establecidas en ellas y que permiten la administración del tráfico y aseguran el acceso, bajo esas condiciones, hacia y desde una red. La aceptación y rechazo se pueden basar en la dirección origen, dirección destino, protocolo de capa superior y números de puerto."*[8]

Lo indicado anteriormente, por el observatorio tecnológico del ministerio de educación, cultura y deporte del gobierno de España, es enfatizado por la Revista de Simulación Computacional, en su artículo titulado Sistema inteligente para validar una lista de control de acceso (ACL) en una red de comunicaciones, donde se indica que, a través del estándar internacional ISO 27002, el cual proporciona un marco de trabajo para los sistemas de gestión de la seguridad de la información (SGSI), *"Las listas de control de acceso (ACL) son un tipo de control que ayuda a definir permisos o accesos según las políticas de seguridad establecidas por la organización y gestionadas por el administrador de la red de comunicaciones."*[9]

Otro punto relevante en la seguridad de los activos de la información, es la asignación de privilegios a los usuario de una red, ya que una mala asignación de privilegios, puede generar eventos de riesgo en la seguridad de la información, como lo pueden ser los accesos no autorizados a dichos activos, esto es mencionado en el artículo reflexivo titulado, gestión de identidades y control de acceso desde una perspectiva organizacional, en el cual se plantea qué: *"Lo que se busca es una solución que permita la asignación efectiva de permisos, dependiendo de las funciones que desempeña cada usuario dentro de la organización."*[10] Teniendo en cuenta lo mencionado, se puede indicar que una política

---

[7] Cano M, Jeimy J y Almanza, Andres. Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018 [En línea]. Bogotá: Revista Ibérica de Sistemas e Tecnologias de Informação, 2020., 477 p. disponible en https://www.researchgate.net/project/Encuesta-Colombiana-de-Seguridad-Informatica

[8] Mifsud, Elvira. Listas de control de acceso (ACL) [En línea]. Madrid: Observatorio tecnológico del ministerio de educación, cultura y deporte del gobierno de España, 2012., disponible en http://recursostic.educacion.es/observatorio/web/gl/software/servidores/1065-listas-de-control-de-acceso-acl?start=3

[9] Hernandez, Talhia. Salazar, Pedro y Soto, Saul. Sistema inteligente para validar una lista de control de acceso (ACL) en una red de comunicaciones [En línea]. Bogotá: Revista de Simulación Computacional, 2017., 24 p. disponible en https://www.ecorfan.org/taiwan/research_journals/Simulacion_Computacional/vol1num2/Revista_de_Simulaci%C3%B3n_Computacional_V1_N2.pdf#page=31

[10] Montoya S, José A y Restrepo R, Zuleima. Gestión de identidades y control de acceso desde una perspectiva organizacional [En línea]. Medellin: Ing. USBMed, 2012., 25 P. disponible en https://dialnet.unirioja.es/descarga/articulo/4694078.pdf

del minino privilegio (PoLP) efectiva debe ser aquella en la que todo lo que no se encuentre permitido de manera expresa en el sistema, debe estar terminantemente prohibido. Las aplicaciones y servicios que no sean estrictamente necesarios deberían ser eliminados de los sistemas informáticos.

Adicionalmente a lo mencionado con anterioridad, se debe considerar que, algunas de las amenazas que se viven diariamente en la seguridad de la información, se pueden deber a los usuarios de red no cuentan con la capacitación necesaria para visualizar los riesgos que infiere hacer un mal uso del sistema, esto es mencionado en el artículo de investigación publicado por el portal web polo del conocimiento titulado La seguridad informática y la seguridad de la información, en el cual se menciona que, *"El acceso solo es permitido a ciertas personas que se encuentren acreditadas, así como su modificación dentro de los límites de su autorización. Las amenazas que se encuentran, son debido a que el propio usuario no tiene en cuenta las vulnerabilidades que existen al hacer un mal uso del sistema. Por ejemplo, al descargar archivos peligrosos o borrar archivos importantes para el sistema. Al mismo tiempo, programas maliciosos como virus o malware."*[11]

2.2.2. PREGUNTA DE INVESTIGACIÓN

¿En qué medida la implementación de listas de control de acceso (ACL), mejora la seguridad de la información en la Empresa CRAWFORD COLOMBIA LTDA?

[11] Figueroa Suárez, Juan A. Rodríguez Andrade, Richard F. Bone Obando, Cristóbal C. y Saltos Gómez, Jazmín A. La seguridad informática y la seguridad de la información [En línea]. Bogotá: Polo del conocimiento, 207., 148 p. disponible en https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

2.2.3. VARIABLES DEL PROBLEMA

Figura 3. *Matriz de variables del problema*

Variable	Dependiente	Independiente	Tipo de Variable	Descripción	Categoría
Controles de seguridad		X	Cualitativa	Ayuda con la regulación de las actividades realizadas sobre los activos de información	Seguridad Lógica
Compromiso de los colaboradores con la seguridad de la información		X	Cuantitativa	Realización de revisiones periódicas a las actividades realizadas por los colaboradores, de acuerdo con los roles determinados	Seguridad Física
Cumplimiento de la normatividad vigente	X		Cuantitativa	Compromiso con el tratamiento responsable de los activos de información, salvaguardando la confidencialidad, integridad y disponibilidad de la información.	Vulnerabilidades / Ataques
Vulnerabilidades en los procesos, relacionados con la seguridad de la información	X		Cualitativa	Revisión de los históricos de las vulnerabilidades reportadas y las acciones correctivas que se han tomado	Vulnerabilidades / Ataques

Figura 3. Matriz de variables del problema

Fuente: Elaboración propia 2021

3. JUSTIFICACIÓN

En la actualidad, las compañías del sector público y del sector privado, han creado una dependencia a sus sistemas de información, lo cual hace que los ciberdelincuentes busquen nuevas estrategias para lograr que sus posibles víctimas entreguen de manera voluntaria información, ya sea personal como corporativa, valiéndose en principio de sitios web y/o correos electrónicos fraudulentos, esto hace que cada vez se preste especial atención a la disponibilidad, confidencialidad e integridad de los activos de la información, para lograr garantizar la correcta prestación de sus servicios, así como la certeza de tener su información segura y sus sistemas protegidos.

Una práctica comúnmente utilizada por los ciberdelincuentes es la ingeniería social, la cual consiste en buscar que los usuarios de red entreguen de manera voluntaria información personal y/o corporativa, la cual puede ser catalogada como información sensible, lo anterior es mencionado en el estudio titulado, Estudio de metodologías de ingeniería social, publicado por la Universidad Oberta de Catalunya: *"el elemento de manipulación social a través de nuestras conductas e intereses en las redes sociales, un camino dorado para el robo de información clave de nuestros productos y vulnera nuestra seguridad, incluso podríamos hablar hasta de nuestra integridad física, toda vez que hay muchos delincuentes informáticos o bandidos que se valen de la huella que dejamos en la red para cometer delitos contra las propiedades o contra las personas."*[12]

Para enfatizar las ventajas de la implementación de las listas de control de acceso (ACL) extendidas, se debe entender que estas ayudan a realizar el filtrado de los paquetes que transitan por la red, ya que solo permiten el tipo de tráfico determinado en la política, desde el router hacia el servidor, adicionalmente realizan el filtrado de las direcciones IP, y este tipo de filtrado puede incluir número de puerto , cualquier tipo de tráfico e IP diferente que pretenda llegar al servidor desde la interfaz del router será denegado, esto es indicado en el libro Managing Cisco Network Security, el cual menciona que "*las listas de control de acceso (ACL) son una forma eficaz de abordar el problema de filtrado mencionado anteriormente. Las ACL son filtros de paquetes que se pueden implementar en routers y dispositivos similares para controlar las direcciones IP de origen y destino que pueden pasar a través de la puerta de enlace. Las listas de acceso extendidas pueden filtrar los protocolos ICMP, IGMP o IP en la capa de red. ICMP se puede filtrar según el mensaje específico."* [13]

Al realizar la observación a la red actual de la empresa CRAWFORD COLOMBIA LTDA., se logra evidenciar que esta se encuentra conformada por cuarenta y cinco equipos conectados bajo una topología tipo estrella y tres servidores distribuidos en tres plantas que se comunican por medio de correos y los archivos que manejan los procesos por VPN, donde todos los equipos están conectados directamente a los switches donde la empresa conecta al router del proveedor UNE, y sus activos de información se encuentran alojados en la nube de Office 365 y en carpetas compartidas desde un servidor físico, para tener acceso en el caso de office 365, es necesario tener una cuenta corporativa con el dominio

[12] Berenguer Serrato, David. Estudio de metodologías de ingeniería social [En línea]. Catalunya: Universidad Oberta de Catalunya, 2018., 5 P. disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

[13] Knipp, Eric. Browne, Brian. Weaver, Woody. Baumrucker, C. Tate. Chaffin, Larry. Caesar, Jamie y Osipov, Vitaly. Managing Cisco Network Security [En línea]. Bogotá: Editorial SYNGRESS, 2020., 13 p. disponible en https://www.elsevier.com/books/managing-cisco-network-security/syngress/978-1-931836-56-2

de la empresa y en el caso de la carpeta compartida, un usuario dentro del dominio de red, al revisar la información almacenada en estos entornos, se evidencia que no se cuenta con restricciones que se encarguen de brindar y denegar acceso a información sensible y que corresponda estrictamente al rol del colaborador en la empresa.

Figura 4. *Red local de la empresa CRAWFORD COLOMBIA LTDA*

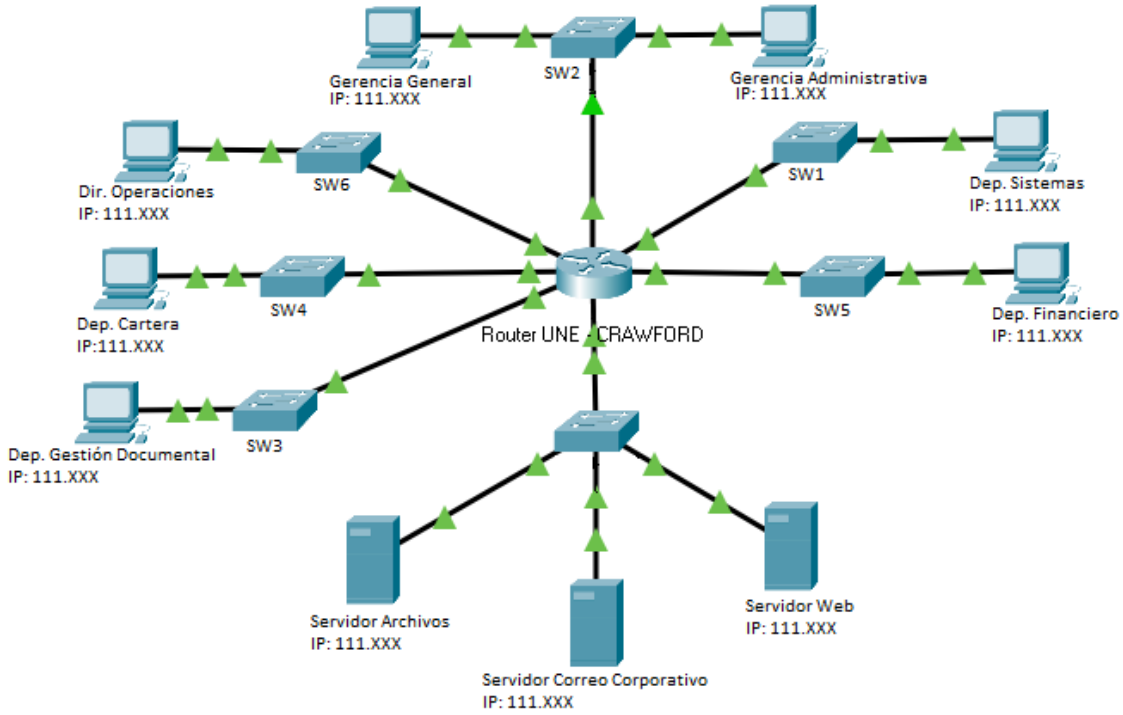

Figura 4. Red local de la empresa CRAWFORD COLOMBIA LTDA

Fuente: Elaboración propia 2021 (Crawford Colombia, 2020)

Conforme a lo expuesto anteriormente y en el planteamiento del problema, se logra evidenciar que, en la actualidad la empresa CRAWFORD COLOMBIA LTDA., presenta algunas falencias relacionadas con la seguridad de la información en sus diferentes áreas, por lo cual se hace necesario verificar las diferentes vulnerabilidades que se puedan presentar en la protección de los datos y los lineamientos de la empresa para asegurar los activos de información, adicionalmente, se hace preciso establecer un modelo de listas de control de acceso (ACL) extendidas, que le permitan a la empresa minimizar los diferentes eventos de riesgo en la seguridad de la información que se puedan presentar, teniendo en cuenta que los activos de información son el insumo indispensable para el normal desarrollo de las actividades diarias de la empresa, realizando un especial enfoque en las políticas de asignación de los roles de los usuarios de red, las cuales, se sugiere, sean basadas en el principio del mínimo privilegio (PoLP), para otorgar los niveles de acceso que sean requeridos por los colaboradores, para cumplir de manera óptima sus actividades diarias, sin copar los recursos de red.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Analizar en qué medida la implementación de listas de control de acceso (ACL), mejora la seguridad, rendimiento y organización de tráfico de datos en la empresa CRAWFORD COLOMBIA LTDA.

4.2. OBJETIVOS ESPECÍFICOS

Describir la situación actual respecto a la seguridad de la información en la empresa CRAWFORD COLOMBIA LTDA.

Realizar una evaluación de los riesgos asociados al control de acceso a la red en la empresa CRAWFORD COLOMBIA LTDA.

Establecer los beneficios de la aplicación de las listas de control de acceso (ACL) y las restricciones a los permisos de los usuarios para acceder a ciertos archivos para reducir las vulnerabilidades en el manejo de la información y la carga de la red en la empresa CRAWFORD COLOMBIA LTDA.

5. MARCOS DE REFERENCIA

Se puede describir una red de datos, como la conexión de un conjunto de periféricos compartiendo recursos. Dichas redes se componen de una parte física, a cual puede contener cables, placas y dispositivos de conexión inalámbrica y una parte lógica la cual, puede estar compuesta por los programas, protocolos de comunicación y sistemas operativos, estas redes tienen como fin, el ahorro en recursos económicos al compartir recursos físicos como lo son las impresoras, se tiene la posibilidad de compartir almacenamiento por lo cual, los equipos no necesitarían grandes capacidades de almacenamiento, se puede lograr la optimización de tiempos al permitir que varios usuarios trabajen sobre el mismo archivo de forma simultánea; adicionalmente se puede administrar la seguridad de los usuarios al asignar permisos y restricciones para controlar el acceso a los recursos de la red, a continuación se listaran algunos trabajos asociados a la seguridad de la información alojada en las redes.

Desde la década de los años sesenta, la estandarización de los protocolos en la comunicación en las redes, ha venido siendo relevante, ya que de esta década datan los primeros estándares en las arquitecturas de protocolos, gracias a estas primeras estandarizaciones, hoy se tiene presente la gran serie de implicaciones que intervienen en la transferencia de datos entre equipos interconectados en una red, adicionalmente gracias a la estandarización se cuenta con un modelo, tanto físico como lógico, para controlar que no se produzcan errores de transmisión de la información, lo anterior es enfatizado en el artículo titulado Redes de computadores, donde se indica: *"desde el principio, se desarrollaron modelos estructurados en niveles: en cada nivel se lleva a cabo una tarea y la cooperación de todos los niveles proporciona la conectividad deseada por los usuarios. Conviene considerar que, en la época que nos ocupa, la informática estaba en manos de muy pocos fabricantes e imperaba la filosofía del servicio integral: cada fabricante lo proporcionaba todo (ordenadores, cables, periféricos, sistema operativo y software)."*[14]

Es importante mencionar que, tanto en los entornos laborales, educativos y/o personales, existe una necesidad por obtener, de una manera rápida, segura y eficiente la información almacenada en los dispositivos que pueden llegar a conformar una red de información, para lograr acceder a dicha información se hace necesario implementar un conjunto de técnicas orientadas a mantener la operatividad, eficiencia y seguridad de una red, manteniéndola constantemente monitoreada y con una planeación adecuada y propiamente documentada, lo cual se entiende como administración de redes de información, de acuerdo con lo mencionado en la publicación de la RISCE Revista Internacional de Sistemas Computacionales y Electrónicos, en el Numero 6, Volumen 3, Año 3, donde se indica que, *"hoy en día, es perfectamente normal hablar de redes en las que conviven dispositivos que no están totalmente conectados a Internet, tales como: teléfonos móviles, PDA's (Personal Digital Assistant), sistemas de navegación para vehículos, consolas de videojuegos, televisión digital; en definitiva, toda una clase de dispositivos heterogéneos. Las tendencias actuales en investigación indican que todos estos dispositivos se conectarán en muy pocos años, a redes con ancho de banda muy superior a lo actual."* [15]

[14] Barceló Ordinas, José María. Íñigo Griera, Jordi. Martí Escalé, Ramón. Peig Olivé, Enric y Perramon Tornil, Xavier. Redes de computadores [En línea]. Catalunya: Universidad Oberta de Catalunya, 2004., 30 p. disponible en https://libros.metabiblioteca.org/bitstream/001/341/9/84-9788-117-6.pdf

[15] RISCE Revista Internacional de Sistemas Computacionales y Electrónicos. Desempeño del Protocolo AODV-

Adicionalmente, las ACL se entienden como un grupo de sentencias que, se utilizan para lograr definir políticas de seguridad de los activos de información que pertenezcan a los dominios seguros al interior de las redes de información, estas políticas definen la forma en las que se van a procesar los paquetes que ingresan a las interfaces de entrada, se reenvían a través del router y los que salen de las interfaces de salida del router, si las ACL no están configuradas en el router, todos los paquetes que pasen a través del router tendrán acceso a todas las partes de la red, lo expuesto anteriormente, se ratifica en el artículo titulado Guía del administrador, donde se menciona que, *"el tipo de política que define quién tiene acceso a un objeto, y que operaciones pueden efectuarse en relación con el mismo, recibe el nombre de política de lista de controles de accesos o política ACL. Las listas de control de acceso (ACL) se utilizan para identificar la política de seguridad de una organización en los recursos que pertenecen al dominio seguro."*[16]

5.1. MARCO CONCEPTUAL

Para lograr la óptima utilización y seguridad de los recursos de red en la empresa CRAWFORD COLOMBIA LTDA, se hace necesario adoptar en todos los niveles y las actividades realizadas diariamente por parte de los colaboradores de la empresa conceptos claves, que permitan el entendimiento y la utilidad de la implementación de listas de control de acceso (ACL).

Algunos de los conceptos más relevantes que se asocian al presente trabajo de investigación son el tratamiento de datos, la finalidad de los datos, la veracidad o calidad de la información, la transparencia en el tratamiento de los datos, el acceso y circulación restringida de la información y la seguridad de la información, ya que estos conceptos se enfatizan en la Ley Estatutaria 1581 de 2012 en su Artículo 4 Literales a al h.

Lo mencionado anteriormente, es complementado con el filtrado de los paquetes que viajan por las redes de información ya que, al lograr regular este tráfico, se puede garantizar que los usuarios accedan a los recursos específicos, esto es expuesto por la Cisco Networking Academy quienes indican que: *"la funcionalidad de ACL típica en el IPv6 es similar a los ACL en el IPv4. Los ACL determinan que trafican para bloquear y que trafican para remitir en las interfaces del switch. Los ACL permiten la filtración basada sobre las direcciones de origen y de destino, entrante y saliente a las interfaces específicas. Cada ACL tiene un enunciado de negación implícito en el extremo. Las reglas para los ACL se configuran en las entradas de control de acceso (ACE)."*[17]

Adicionalmente, garantizar la seguridad de la información se ha convertido en una de las principales tareas de las empresas, por lo que recurren a herramientas que les permita

---

CDMA para Redes Ad-Hoc [En línea]. Bogotá: Instituto politecnico nacional, 2011., 7 p. disponible en https://www.uaeh.edu.mx/investigacion/icbi/LI_FisMat/itza_ortiz/RISCENoviembre2011.pdf

[16] Trivoli Software. Guía del administrador [En línea]. Bogotá: Publib boulder, 2006., disponible en http://publib.boulder.ibm.com/tividd/td/ITAME/GC23-4684-00/es_ES/HTML/adminmst06.htm

[17] Cisco Networking Academy. Lista de control de acceso (ACL) y Entrada de control de acceso (ACE) de la configuración IPv6-based en un Switch [En línea]. California: Cisco, 2018., disponible en https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-350-series-managed-switches/smb3050-configure-ipv6-based-access-control-list-acl-and-access-cont.html

verificar la seguridad de la información, una de estas herramientas es el estándar internacional ISO 27001, en la cual se indica la: *"gestión del acceso de usuarios objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información."*[18]

Figura 5. *Control de acceso*

Registro de usuarios.	**Control:** Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.
Gestión de privilegios.	**Control:** Se debe restringir y controlar la asignación y uso de privilegios
Gestión de contraseñas para usuarios.	**Control:** La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.
Revisión de los derechos de acceso de los usuarios.	**Control:** La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.

Figura 5. Control de acceso

Fuente: Estándar Internacional ISO 27001 (ICONTEC, 2006)

Para complementar lo mencionado anteriormente, se hace importante que al interior de las organizaciones logren identificar sus propias fuentes de riesgo, que las puede originar y cuál sería el impacto, esta identificación puede ser generada mediante una lista completa, donde se relacionen los riesgos basados en eventos que tienen la capacidad de crear, aumentar, evitar, reducir, acelerar o retrasar el logro de sus objetivos, esto es contemplado en el estándar internacional ISO 27005, el cual hace un gran acercamiento a la gestión del riesgo al indicar que: *"el propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir está perdida."*[19]

Es importante resaltar que, en las redes se pueden encontrar diferentes medidas, entre las cuales, se puede destacar el separar el tráfico mediante VLANs, para que la red quede

[18] Instituto Colombiano de Normas Técnicas y Certificación. Estándar internacional ISO 27001 [En línea]. Bogotá: ICONTEC, 2006., 24 p. disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

[19] Instituto Colombiano de Normas Técnicas y Certificación. Estándar internacional ISO 27005 [En línea]. Bogotá: ICONTEC, 2008., 12 p. disponible en http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107

acotada a un único segmento lógico. En la presente investigación se pretende trabajar al nivel de las capas 3 y 4, capa de red y capa de transporte del modelo OSI, ya que las ACLs permiten que sean los propios equipos de red los que permitan o denieguen cierto tipo de comunicaciones antes de llegar a los firewalls.

Teniendo en cuenta los conceptos mencionados anteriormente, junto con el adecuado análisis de la configuración de las listas de control de acceso (ACL), se puede mejorar la seguridad de la información, el rendimiento y la organización del tráfico de datos de las empresas en las cuales se implemente.

5.2. MARCO TEÓRICO

Todos los recursos y políticas enfocados a la seguridad en la información han tenido un gran impacto a lo largo del tiempo, ya sean en empresas pequeñas, medianas o grandes, toda vez que, la implementación de estos repercute directamente en los recursos de las empresas, es de vital importancia el entender que los riesgos en seguridad de la información, deben ser contemplados en función de los agentes de amenazas que sean aplicables a su nicho de negocio especifico, una acertada introducción a la seguridad de la información, es la realizada por OWASP Top 10 de 2017, la cual indica que, *"cada organización es única, y también lo son los agentes de amenaza para esa organización, sus objetivos y el impacto de cualquier brecha. Si una organización de interés público utiliza un sistema de gestión de contenido (CMS) para manipular información pública y el sistema de salud utiliza el mismo CMS para tratar datos sensibles, los agentes de amenaza y los impactos en el negocio son muy distintos para el mismo software."*[20]

Un punto de vista bastante acertado en materia de seguridad de la información, es el indicado por el blog de seguridad informática Cybereop en su revista de Seguridad para PYMES, al indicar que, *"para una pyme, las medidas de ciberseguridad que se tomen son fundamentales, ya que, los ciberdelincuentes están concentrando sus ataques en ellas debido a la falta de inversión o de herramientas de seguridad, lo que provoca un aumento de las vulnerabilidades."*[21]

Se hace importante resaltar el papel que juega el usuario interno como principal responsable en el manejo de los activos de la información y en algunos casos, el vector principal en las vulnerabilidades en los sistemas de seguridad de la información, esto teniendo en cuenta que, la mayoría de usuarios no cuentan con las capacitaciones necesarias en seguridad de la información, lo cual supone una gran brecha en la seguridad de la información al interior de las organizaciones, lo anterior, es mencionado en el artículo publicado por la Europapress en su portal TIC en la sección de Ciberseguridad, titulado La peor vulnerabilidad contra la ciberseguridad de las empresas: el usuario, en el cual indican que, *"tenemos algún caso reciente en empresas de gran prestigio, en el que alguno de estos usuarios ha sido el encargado de "abrir la puerta" a los diferentes ataques que se han producido en las mismas y, en la mayoría de los casos, sin ser conscientes de ello y*

[20] Open Web Application Security Project. OWASP Top 10 - 2017 [En línea]. Bogotá: OWASP, 2017., 5 p. disponible en https://owasp.org/www-pdf-archive/OWASP-Top-10-2017-es.pdf

[21] Cybereop. Seguridad para PYMES [En línea]. Bogotá: Cybereop, s.f., disponible en https://www.cybereop.com/blog/te-presentamos-nuestra-revista-ciberseguridad-pyme.html

produciendo pérdidas millonarias para las compañías. Un ejemplo lo tenemos en el caso de WannaCry, 'ransonware' que afectó a grandes empresas el pasado mes de mayo."[22], este tipo de malware se aprovecha de vulnerabilidades especificas en los sistemas de información, para expandirse por las redes de las empresas, pero se debe tener en cuenta que en muchos casos el foco de infección principal fue un usuario.

Para enfatizar lo mencionado anteriormente, es importante realizar un enfoque al sistema de gestión de la seguridad de la información, desde la visión del estándar internacional ISO 27001 el cual indica que, *"el diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización."*[23]

Teniendo en cuenta lo anterior, se puede indicar que, un sistema de gestión de la seguridad de la información, consiste en un enfoque metódico para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio.

De manera complementaria, el estándar internacional ISO 27005, hace un acercamiento a la gestión del riesgo de las TI, al indicar que, *"los criterios de evaluación del riesgo utilizados para tomar decisiones deberían ser consistentes con el contexto definido para la gestión del riesgo en la seguridad de la información externa e interna y deberían tomar en consideración los objetivos de la organización, los puntos de vista de las partes interesadas."*[24]

Adicionalmente, se hace necesario visibilizar las vulnerabilidades en la informática, lo cual se entiende, de acuerdo con el portal web del Instituto Nacional de Ciberseguridad, como *"una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos."*[25]

---

[22] Saavedra, Fernando. La peor vulnerabilidad contra la ciberseguridad de las empresas: el usuario [En línea]. Madrid: Europapress, 2017., disponible en https://www.europapress.es/portaltic/ciberseguridad/noticia-peor-vulnerabilidad-contra-ciberseguridad-empresas-usuario-20171124140136.html

[23] Instituto Colombiano de Normas Técnicas y Certificación. Estándar internacional ISO 27001 [En línea]. Bogotá: ICONTEC, 2006., I p. disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

[24] Instituto Colombiano de Normas Técnicas y Certificación. Estándar internacional ISO 27005 [En línea]. Bogotá: ICONTEC, 2008., 21 p. disponible en http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107

[25] INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [En línea]. Bogotá: Instituto Nacional de Ciberseguridad, 2017., disponible en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

Para lograr un acercamiento más preciso a las vulnerabilidades en la informática, se puede indicar que, los sistemas operativos, los navegadores web y otros programas que se pueden descargar de la web, en gran medida integran problemas de seguridad, los cuales pueden ser aprovechados por los ciberdelincuentes para lograr ingresar a las PC y lograr sustraer información.

Para lograr robustecer aún más la seguridad de la información, se hace necesario realizar una mención de las listas de control de acceso (ACL), las cuales permiten indicarle al router cuáles son los tipos de paquetes que se deben aceptar o rechazar, estas acciones se basan en condiciones específicas y permiten que la administración del tráfico de una red se realice de manera segura, esto al permitir o negar que los usuarios de la red puedan acceder a recursos epecificos, esto es enfatizado en el artículo titulado Lista de control de acceso (ACL) y Entrada de control de acceso (ACE) de la configuración IPv6-based en un Switch, el cual indica que, *"un ACL contiene los hosts que permiten o niegan el acceso al dispositivo de red. La funcionalidad de ACL típica en el IPv6 es similar a los ACL en el IPv4. Los ACL determinan que trafican para bloquear y que trafican para remitir en las interfaces del switch. Los ACL permiten la filtración basada sobre las direcciones de origen y de destino, entrante y saliente a las interfaces específicas. Cada ACL tiene un enunciado de negación implícito en el extremo. Las reglas para los ACL se configuran en las entradas de control de acceso (ACE)."*[26]

5.3. MARCO JURÍDICO

Como un estado de derecho, a través de los años, Colombia se ha comprometido con el tratamiento responsable de los activos de información, sancionado Leyes, Decretos, Resoluciones y diversas pronunciaciones de carácter jurídico, buscando garantizar la confidencialidad, integridad y disponibilidad de la información, dándole herramientas a las personas naturales y/o jurídicas, para actuar de una manera eficaz, al momento de ser responsables del tratamiento de los activos de información y/o ser víctimas de ataques a los mismos.

Ley Estatutaria 1581 de 2012, la cual tiene como objeto *"desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."*[27]

Así pues, se analiza con mayor énfasis el Artículo 4 Literales a al h de la Ley Estatutaria 1581 de 2012, donde se presentan los principios fundamentales que se deben aplicar de manera armónica e integral, para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

[26] Docplayer. Lista de control de acceso (ACL) y Entrada de control de acceso (ACE) de la configuración IPv6-based en un Switch [En línea]. Bogotá: Docplayer, 2020., disponible en http://docplayer.es/186386951-Lista-de-control-de-acceso-acl-y-entrada-de-control-de-acceso-ace-de-la-configuracion-ipv6-based-en-un-switch.html

[27] Congreso de la República de Colombia. Ley Estatutaria 1581 de 2012 [En línea]. Bogotá: Congreso de la República de Colombia, 2012., 1 p. disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

De igual manera se analiza la **Ley Estatutaria 1266 de 2008,** *"por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."*[28]

De acuerdo con lo anterior, se analiza de manera detallada el Artículo 3 Literales a al j de la Ley Estatutaria 1266 de 2008, el cual menciona las definiciones de titular de la información, fuente de información, operador de información, usuario, dato personal, dato público, dato semiprivado, dato privado, agencia de información comercial e información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Igualmente se analiza la **Ley 1273 de 2009,** la *"cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."*[29]

De la Ley 1273 de 2009, se resalta el Título I Artículos 269A al 269H, en los cuales se detallan las penas y sanciones en la cuales se pueden incurrir, si se atenta contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Teniendo en cuenta que le empresa CRAWFORD COLOMBIA LTDA, pertenece al sector financiero, es importante analizar la **Ley 1328 de 2009** la cual, *"tiene por objeto establecer los principios y reglas que rigen la protección de los consumidores financieros en las relaciones entre estos y las entidades vigiladas por la Superintendencia Financiera de Colombia, sin perjuicio de otras disposiciones que contemplen medidas e instrumentos especiales de protección."*[30]

Se hace necesario contemplar los Títulos I al V, de la Ley 1328 de 2009, debido a que, estos títulos hacen mención a conceptos claves a tener en cuenta como lo son, los aspectos generales pertenecientes al régimen financiero, los derechos y obligaciones, el sistema de atención al consumidor financiero, la información al consumidor financiero y las cláusulas y prácticas abusivas.

---

[28] Congreso de la República de Colombia. Ley Estatutaria 1266 de 2008 [En línea]. Bogotá: Congreso de la República de Colombia, 2008., 1 p. disponible en http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf

[29] Congreso de la República de Colombia. Ley 1273 de 2009 [En línea]. Bogotá: Congreso de la República de Colombia, 2009., 1 p. disponible en https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[30] Congreso de la República de Colombia. Ley 1328 de 2009 [En línea]. Bogotá: Congreso de la República de Colombia, 2009., 1 p. disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=36841

5.4. ESTADO DEL ARTE

Las amenazas a los sistemas de información evolucionan diariamente, por lo cual, se hace necesario que las acciones preventivas, para salvaguardar los activos de información, evolucionen a la misma velocidad que las posibles amenazas, teniendo en cuenta esta creciente evolución en los ataques a la seguridad de la información , también es relevante hacer una mención a lo indicado por el Open Web Application Security Project, el cual indica que, *"hemos rediseñado completamente el OWASP Top 10, mejorado la metodología, utilizado un nuevo proceso de obtención de datos, trabajamos con la comunidad, reordenamos los riesgos y los reescribimos desde cero, y agregamos referencias a frameworks y lenguajes que son utilizados actualmente En los últimos años, la tecnología base y la arquitectura de las aplicaciones ha cambiado significativamente."*[31]

Al realizar una comparación, hace aproximadamente 40 años, el acceso a la información en la internet era muy limitada y solo una pequeña parte de la población mundial podría tener este acceso a la información allí, tengamos en cuenta que, la información no estaba tan conectada o globalizada como lo está hoy en día, por lo que la seguridad de la información se basaba únicamente en entornos físicos y no lógicos.

Ahora en este nuevo milenio el transporte de toda la información se torna un poco más compleja para que pueda ser global y esté al alcance de cualquier persona que desee acceso a la información, pero con este nuevo alcance atrae nuevos retos.

Se debe tener en cuenta que, la evolución que se ha vendo evidenciando en los últimos años, en materia de seguridad de la información, no es un evento reciente, ya que desde los inicios de la década de 2000 los ciberdelincuentes explotaban vulnerabilidades que se detectaban en los sistemas operativos, hardware y aplicaciones, lo cual conllevo a que las empresas combinaran herramientas de seguridad como lo son los firewalls y antivirus para proteger los sistemas de los ciberataques, adicionalmente buscaban nuevas formas para que fueran los mismos usuarios de red, quienes revelaran información, de manera voluntaria, apoyándose en ataques de ingenieria social, lo anterior es enfatizado en el portal web de la empresa CyberSecurity quienes indican que, *"la protección proporcionada comenzó a caer frente a la velocidad a la que los ataques evolucionaban en sofisticación e impacto. Comenzaban a aparecer ataques dirigidos a las herramientas encargadas de proteger la información y la red corporativa. El uso de las redes sociales comienza a extenderse de forma masiva. Por otro lado, empiezan a producirse los riesgos de seguridad derivados de empleados insatisfechos y los fraudes online."*[32]

Algunos ataques, como la piratería digital, no se dieron de la noche a la mañana, sino que requirieron del trabajo de hackers que descubrieron y explotaron las vulnerabilidades críticas de los sistemas y expusieron debilidades claves, uno de estos casos es el de el hacker Adrian Lamo, quien, mediante la utilización de una herramienta de administración de contenido, la cual no se encontraba protegida en Yahoo, pudo modificar un artículo de

[31] Open Web Application Security Project. OWASP Top 10 - 2017 [En línea]. Bogotá: OWASP, 2017., 4 p. disponible en https://owasp.org/www-pdf-archive/OWASP-Top-10-2017-es.pdf

[32] CyberSecurity. Cómo ha evolucionado la ciberseguridad en los últimos 25 años y cómo ha sido la evolución de seguridad en las empresas [En línea]. Bogotá: hard2bit, 2019., disponible en https://hard2bit.com/blog/como-ha-evolucionado-la-ciberseguridad-en-los-ultimos-25-anos-y-como-ha-sido-la-evolucion-de-seguridad-en-las-empresas/

Reuters y agregar una cita falsa atribuida al exfiscal general John Ashcroft, este evento, se encuentra documentado en el portal web Kaspersky.com, en su artículo titulado los 10 hackers más infames de todos los tiempos, en el cual adicionalmente mencionan que, "*Lamo fue demasiado lejos cuando pirateó la intranet de The New York Times, se incluyó en la lista de fuentes expertas, y comenzó a realizar investigaciones sobre personajes públicos de alto perfil. Como prefería circular por las calles llevando solo una mochila y no poseía una dirección fija, Lamo se ganó el apodo de "El hacker indigente".*"[33]

Otro evento relevante en la seguridad de la información se originó en el año 2003 cuando nace una de las organizaciones más importantes en lo que respecta a ataques cibernéticos conocida como Anonymous la cual está conformada por personas del común y las cuales se aprovechan de vulnerabilidades en los sistemas de información, para lograr tener acceso a información de carácter clasificada y/o reserva, esto para lograr generar daños a personas naturales y/o jurídicas y causar daños a los intereses públicos.

A la par de los eventos mencionados anteriormente, Colombia se ha comprometido con el tratamiento responsable de los activos de información, sancionado Leyes, Decretos, Resoluciones y diversas pronunciaciones de carácter jurídico, algunas de estas normas son la ley de hábeas data (Ley 1266 de 2008), ley contra los delitos informáticos (Ley 1273 de 2009), ley protección al consumidor financiero (Ley 1328 de 2009) y la ley de protección de datos personales (Ley 1581 de 2012).

Para enfatizar el compromiso que Colombia ha venido teniendo con la seguridad de la información, se puede verificar el documento Conpes 3701 de 2011 publicado por el Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación, en el cual el Gobierno Nacional, precisa conocer y actuar de forma completa frente a las amenazas informáticas o incidente informático que puedan comprometer información, afectar la infraestructura crítica del país y poner en riesgo la seguridad y defensa del Estado, esto mediante una estrategia integral que abarque la creación de instancias adecuadas que permitan ejercer una labor de ciberseguridad y ciberdefensa frente a cualquier amenaza, *"es de vital importancia crear conciencia y sensibilizar a la población en todo lo referente a la seguridad de la información; fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques."*[34], para adelantar la implementación del Conpes 3701, se definieron tres objetivos específicos, los cuales contemplan la implementación de las instancias apropiadas para lograr proteger la infraestructura crítica nacional, el diseño y ejecución de planes de capacitación especializada en ciberseguridad y ciberdefensa y el fortalecimiento del cuerpo normativo y de cumplimiento en la materia.

Adicionalmente, a la puesta en marcha del documento Conpes 3701 de 2011, el estado colombiano ha realizado otro gran avance en materia de ciberseguridad, al depositar ante el Consejo de Europa, el día 16 de marzo de 2020, el instrumento de adhesión al Convenio de Budapest, que es el estándar mundial en la lucha contra la ciberdelincuencia el cual,

[33] Kaspersky. Los 10 hackers más infames de todos los tiempos [En línea]. Bogotá: Kaspersky, s.f., disponible en https://latam.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

[34] Consejo Nacional de Política Económica y Social. Conpes 3701 [En línea]. Bogotá: Consejo Nacional de Política Económica y Social, 2011., 20 p. disponible en https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

"consciente de la necesidad de mejorar la coordinación y la cooperación entre los Estados, así como fortalecer las capacidades nacionales, con el fin de prevenir, detectar, investigar y enjuiciar a la delincuencia organizada transnacional en el ciberespacio, nuestro país adhiere al Convenio de Budapest con las siguientes expectativas: - Actualizar y complementar la legislación nacional a los estándares internacionales contra la ciberdelincuencia."[35]

Tomando en consideración lo mencionado con anterioridad, se crea la necesidad de reforzar todos los entornos informáticos en aras de la protección de la información, por lo cual nace el estándar internacional ISO 27001, el cual establece los requisitos para implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, *"esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. La adopción del modelo PHVA también reflejará los principios establecidos en las Directrices OCDE (2002)1 que controlan la seguridad de sistemas y redes de información."*[36] El estándar ofrece un modelo completo de principios y directrices, que se sugieren implementar, para adelantar la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

Figura 6. *Modelo PHVA aplicado a los procesos de SGSI*

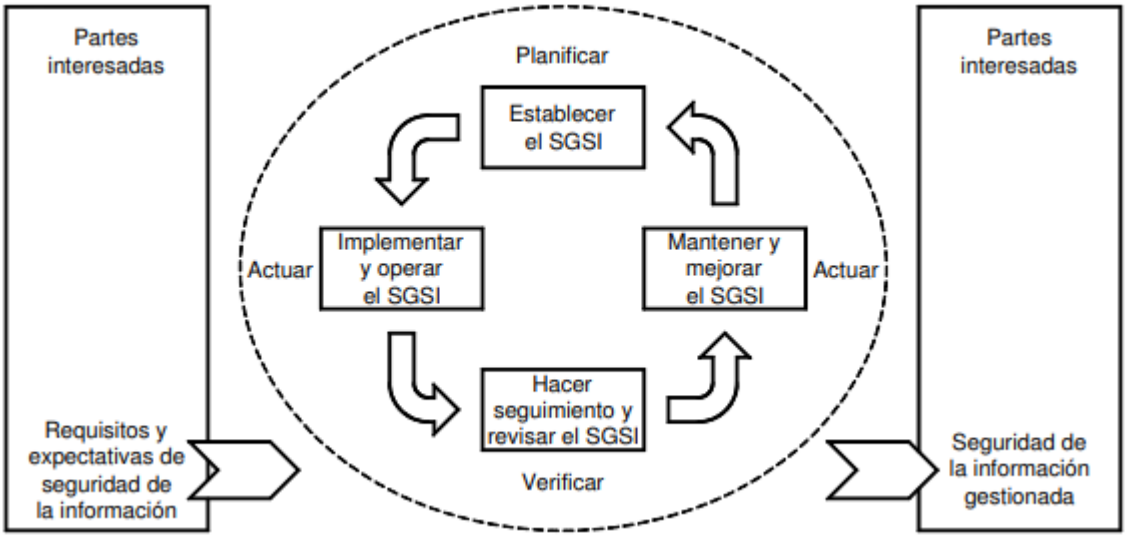

Figura 6. Modelo PHVA aplicado a los procesos de SGSI

Fuente: Estándar Internacional ISO 27001 (ICONTEC, 2006)

[35] Cancillería de Colombia. Colombia se adhiere al Convenio de Budapest contra la ciberdelincuencia [En línea]. Bogotá: Cancillería de Colombia, 2020., disponible en https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

[36] Instituto Colombiano de Normas Técnicas y Certificación. Estándar internacional ISO 27001 [En línea]. Bogotá: ICONTEC, 2006., II p. disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

6. METODOLOGÍA

6.1. FASES DEL TRABAJO DE GRADO

Figura 7. *Fases del trabajo de grado*

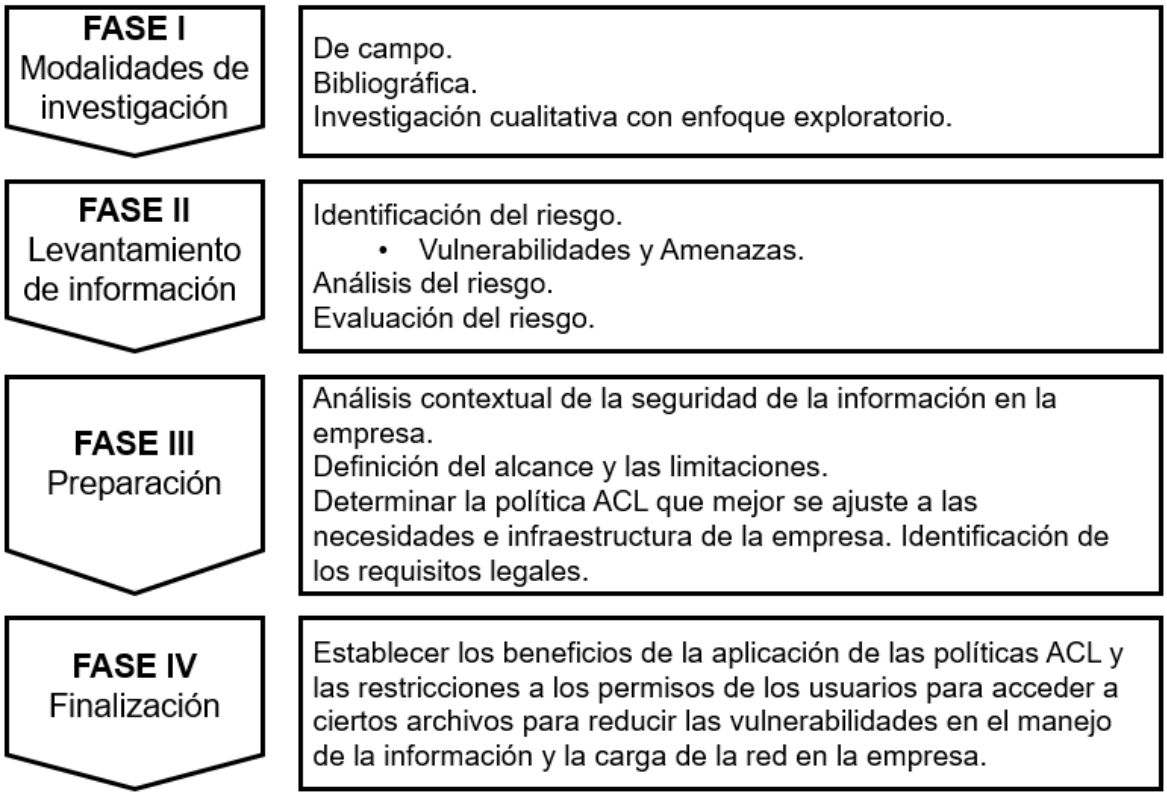

Figura 7. Fases del trabajo de grado

Fuente: Elaboración propia 2021

En fase I se logra establecer que, para la presente investigación se requiere un enfoque exploratorio - cualitativo, ya que con este tipo de investigación se puede llegar a conocer de una manera más detallada todas las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas, evidenciadas en el desarrollo de las políticas de seguridad informática, en las operaciones de la empresa CRAWFORD COLOMBIA LTDA.

En la fase II se logra determinar que, en la actualidad ha tomado gran importancia que las organizaciones logren identificar de manera oportuna las posibles fuentes de riesgo, sus causas y consecuencias. Es importante que se trace como objetivo el detallar una lista con los posibles riesgos, basándose en los eventos que tienen la capacidad de crear, aumentar, evitar, reducir, acelerar o retrasar el logro de los objetivos del negocio, es recomendable que la identificación se realice de tal manera que sea posible conocer y determinar los eventos que puedan tener un potencial para causar pérdida.

Figura 8. *Posición de la fase de análisis del riesgo en el proceso de gestión del riesgo*

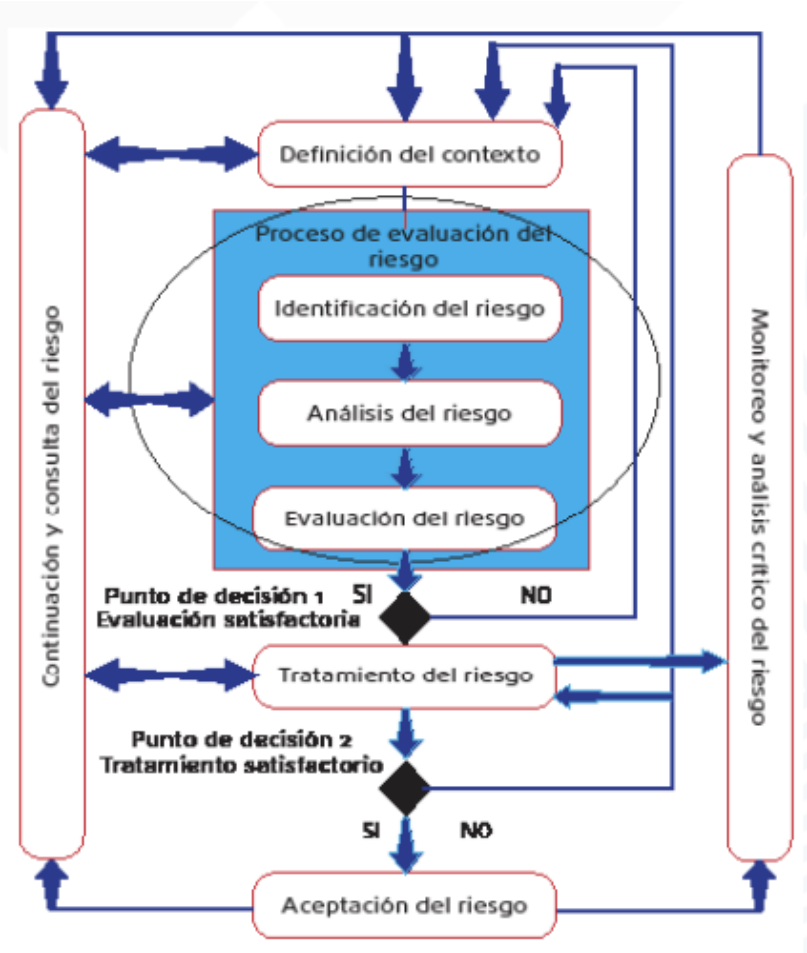

Figura 8. Posición de la fase de análisis del riesgo en el proceso de gestión del riesgo

Fuente: Estándar Internacional ISO 27005 (ICONTEC, 2008)

En las fases III y IV se puede indicar que, las ACL pueden definirse sin aplicarlas. Para crear una ACL operativa y activa, la ACL debe aplicarse a la interfaz del router. Las ACL extendidas permiten que el administrador de la red acceda o deniegue el tráfico que fluye desde un puerto o unas direcciones IP específicas hasta un puerto o direcciones IP de destinos dados. Esta capacidad permite al administrador de la red ser mucho más específico en lo referente al tráfico que puede pasar por la red. Las ACL extendidas deben aplicarse a la interfaz más cercana al origen del tráfico. Para bloquear el tráfico de un origen hacia un destino específico, se emplea una ACL entrante a E0 del router A en lugar de una lista saliente a E1 del router C.

Figura 9. *Número de las listas de acceso CISCO IOS*

Listas de acceso	Descripción del número
1 a 99	Lista de acceso IP estándar
100 a 199	Lista de acceso IP extendida
200 a 299	Lista de acceso de protocolo de tipo código
300 a 399	Lista de acceso DECnet
400 a 499	Lista de acceso estándar XNS
500 a 599	Liste de acceso extendida XNS
600 a 699	Lista de acceso AppleTalk
700 a 799	Lista de acceso de dirección MAC de 48 bits
800 a 899	Lista de acceso estándar IPX
900 a 999	Lista de acceso extendida IPX
1000 a 1099	Lista de acceso IPX SAP
1100 a 1199	Lista de acceso de dirección MAC de 48 bits extendida
1200 a 1299	Lista de acceso de dirección resumida IPX
1300 a 1999	Lista de acceso estándar IP(intervalo expandido)
2000 a 2699	Lista de acceso extendida IP (intervalo expandido)

Figura 9. Número de las listas de acceso CISCO IOS

Fuente: Configuración de Listas de Acceso IP (Cisco, 2007)

6.2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

HERRAMIENTAS DE RECOLECCIÓN DE INFORMACIÓN.

Figura 10. *Matriz de herramientas utilizadas*

Cod	Objetivo	Descripción	Herramientas
1	Describir la situación actual respecto a la seguridad de la información en la empresa Crawford Colombia LTDA.	Determinar la metodología de la investigación.	1. Investigación de campo. 2. Revisión bibliográfica. 3. Investigación cualitativa con enfoque exploratorio.
2	Realizar una evaluación de los riesgos asociados al control de acceso a la red en la empresa Crawford Colombia LTDA.	Realizar un análisis intuitivo de los riesgos que se pueden derivar de una determinada actividad.	1. OWASP Top 10 2017. 2. Matriz DOFA. 3. Matriz PESTEL + Porter. 4. Matriz Gestión del Riesgo. 5. Matriz Poder-Interés.
3	Establecer los beneficios de la aplicación de las políticas ACL y las restricciones a los permisos de los usuarios para acceder a ciertos archivos para reducir las vulnerabilidades en el manejo de la información y la carga de la red en la empresa Crawford Colombia LTDA.	Los estándares internacionales y las matrices, ayudan a gestionar la seguridad de la información en una organización.	1. ISO 27001. 2. ISO 27005. 3. Análisis y Utilización de las matrices. 4. Configuración de Listas de Acceso IP. 5. OWASP Top 10 2017.

Figura 10. Matriz de herramientas utilizadas

Fuente: Elaboración propia 2021

Para realizar la descripción de la situación actual respecto a la seguridad de la información en la empresa CRAWFORD COLOMBIA LTDA, se utiliza la investigación cuantitativa ya que, mediante la utilización de este tipo de investigación, se puede recolectar y analizar datos, mediante la utilización de herramientas como lo son la observación y las entrevistas a los participantes, de acuerdo con lo planteado en el artículo Investigación: Investigación cuantitativa y cualitativa, se puede determinar que, *"la investigación cuantitativa trata de determinar la fuerza de asociación o correlación entre variables, la generalización y objetivación de los resultados a través de una muestra para hacer inferencia a una población de la cual toda muestra procede. Tras el estudio de la asociación o correlación pretende, a su vez, hacer inferencia causal que explique por qué las cosas suceden o no de una forma determinada."*[37]

Adicionalmente la revisión bibliográfica, es otra herramienta, que brinda una gran utilidad al desarrollo del presente trabajo de investigación, ya que se trata de la búsqueda de información a través de la consulta de libros, revistas, investigaciones, informaciones, documentos, escritos, estadísticas, mapas periódicos, obras literarias, con lo cual se puede realizar un acercamiento a la realidad, adicionalmente *"no basta simplemente con parafrasear o resumir fielmente las ideas de otros textos, es necesario comentar, cuestionar, interrogar lo que dicen."*[38]

Para adelantar la evaluación de los riesgos asociados al control de acceso a la red en la empresa CRAWFORD COLOMBIA LTDA, la utilización de matrices es una herramienta esencial ya la que es un instrumento utilizado para mejorar el control de riesgos y la seguridad de una organización, *"por lo tanto, es un instrumento válido para mejorar el control de riesgos y la seguridad de una organización. A través de este instrumento se puede realizar un diagnóstico objetivo y global de empresas de diferentes tamaños y sectores de actividad. Asimismo, mediante la matriz de riesgo es posible evaluar la efectividad de la gestión de los riesgos, tanto financieros como operativos y estratégicos, que están impactando en la misión de una determinada organización."*[39]

Teniendo en cuenta que con las listas de control de acceso (ACL) extendidas, se puede permitir o rechazar el acceso a ciertos paquetes de datos según su destino o su origen, adicionalmente permite configurar varias restricciones en una sola ACL, es recomendable que se tenga un estándar en las nomenclaturas de las listas de control de acceso (ACL), puertos y listas de acceso a crear, también el lugar donde se ubique una ACL ya que influye en la reducción del tráfico de datos y su óptimo funcionamiento dentro de la organización.

De acuerdo a lo establecido anteriormente, se puede validar que las configuraciones de las listas de control de acceso (ACL), ayudarán a mejorar el rendimiento de la red y servidores de la empresa CRAWFORD COLOMBIA LTDA, reduciendo y controlando de manera considerable el tráfico de datos de la organización, esto se verá reflejado en un óptimo

[37] Pita Fernández, S y Pértegas Díaz, S. Investigación: Investigación cuantitativa y cualitativa [En línea]. Coruña: Fisterra, 2002., 1 p. disponible en https://www.fisterra.com/mbe/investiga/cuanti_cuali/cuanti_cuali2.pdf
[38] Peña, Luis Bernardo. PROYECTO DE INDAGACIÓN La revisión bibliográfica [En línea]. Bogotá: Pontificia Universidad Javeriana, 2010., disponible en https://www.javeriana.edu.co/prin/sites/default/files/La_revision_bibliografica.mayo_.2010.pdf
[39] ISOTools. ¿En qué consiste una matriz de riesgos? [En línea]. Bogotá: ISOTools, 2015., disponible en https://www.isotools.org/2015/08/06/en-que-consiste-una-matriz-de-riesgos/

control de las directivas ya que se regulan de manera eficiente las operaciones realizadas al interior de la organización.

Respecto a los roles y permisos de acceso con los que cuentan los colaboradores de la empresa CRAWFORD COLOMBIA LTDA, para accesar a los recursos de red, se logra establecer la importancia de contar con una política de creación de usuarios con mínimos privilegios (principio del mínimo privilegio (PoLP) y de acuerdo con los niveles de responsabilidad acordes a cada cargo, se den los privilegios de acceso a los recursos y a los activos de información que reposan en los servidores y carpetas de red de la empresa, ya que como se ha mencionado anteriormente, para tener acceso, en el caso de office 365 es necesario tener una cuenta corporativa con el dominio de la empresa y en el caso de la carpeta compartida un usuario dentro del dominio de red.

6.3. ALCANCES Y LIMITACIONES

El proyecto se centra en buscar las mejores políticas de seguridad ACL que se acoplen a la empresa en mención, con el fin de proteger la información del personal y de la compañía en general, investigando a través de un enfoque cualitativo permitiendo el descarte de aquellas ACL que no sean necesarias implementar.

Esto incluye:

Acceso a la computadora: El administrador de seguridad debe configurar todos los equipos de cómputo, para que estos sólo puedan ser utilizados por los colaboradores cuyos datos de usuario y contraseña hayan sido previamente registrados en el sistema.

Acceso a la red: teniendo en cuenta que la conexión de red interna de la compañía se encuentra basada en cableado estructurado, a través del directorio activo se debe garantizar que únicamente los colaboradores que cuenten con las debidas autorizaciones puedan acceder a la red de la compañía a través de mecanismos de autentificación.

Cuenta de usuario: El directorio activo asigna a todos los colaboradores de la empresa una única cuenta de usuario y contraseña que les permita acceder a la red de la compañía.

Roles y permisos de acceso: El administrador de seguridad debe configurar en el directorio activo todas las cuentas de usuario teniendo en cuenta el principio del mínimo privilegio (PoLP), y de acuerdo con los niveles de cada cargo, se deben dar los privilegios de acceso a la red.

Registro de Actividades: Se debe tener un registro de las actividades por medio de la creación de una directiva de auditoria en el directorio activo de los usuarios en la red para posteriormente detectar anomalías que puedan ser potencialmente peligrosas para la compañía.

Restricción a Sitios de Internet: Únicamente los empleados autorizados pueden hacer uso de internet y los mismos no podrán visitar sitios web que puedan incurrir en la seguridad de

la empresa o que estén en contra de la estrategia laboral de la compañía, por lo que se recomienda hacer la adquisición de un firewall físico

Correo Electrónico: Los empleados no deberán ejecutar ningún archivo que pueda ser catalogado como (SPAM) o que provenga de personas desconocidas, no deberán suministrar sus datos de usuario y contraseña, así como tampoco sacar información de la compañía debido a que podrían ser víctimas de phishing.

7. PRODUCTOS A ENTREGAR

Trabajo de grado donde se incluye la descripción de la situación actual respecto a la seguridad de la información, una evaluación de riesgos asociados al control de acceso a la red y los beneficios de la aplicación de las listas de control de acceso (ACL) y las restricciones a los permisos de los usuarios para acceder a ciertos archivos para reducir las vulnerabilidades en el manejo de la información y la carga de la red en la empresa CRAWFORD COLOMBIA LTDA.

Artículo IEEE.

8. ENTREGA DE RESULTADOS E IMPACTOS

El descubrimiento de las vulnerabilidades es importante, pero ser capaz de estimar el riesgo asociado para el negocio es igualmente importante. Al principio del ciclo de vida, se pueden identificar problemas de seguridad en la arquitectura o el diseño mediante el uso de modelos de amenazas. Más tarde, se puede encontrar problemas de seguridad mediante la revisión del código o las pruebas de penetración. O bien, es posible que los problemas no se descubran hasta que la aplicación esté en producción y en realidad esté comprometida.

Para lograr establecer los beneficios de la aplicación de las listas de control de acceso (ACL) y las restricciones a los permisos de los usuarios para acceder a ciertos archivos para reducir las vulnerabilidades en el manejo de la información y la carga de la red en la empresa CRAWFORD COLOMBIA LTDA, según la observación realizada a la infraestructura de la empresa, el tipo de ACL que se ajusta más a dicha infraestructura, es la lista de acceso IP extendida, ya que las listas de control de acceso (ACL) extendidas filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.

El impacto deseado mediante la ejecución del presente trabajo, es que la empresa CRAWFORD COLOMBIA LTDA cumpla con amplios criterios en sus procesos de resguardo de los activos de información y que el aseguramiento de los mismos, mediante la implementación de listas de control de acceso (ACL) extendidas, ya que estas permiten otorgar o denegar el acceso según la dirección IP, bien sea la dirección de origen, la dirección de destino, el tipo de protocolo y los números de puertos.

En la matriz de riesgos que se presenta en la evaluación del riesgo, se pretende mostrar e identificar los riesgos potenciales a los que se encuentran expuestos los activos de la información de la empresa CRAWFORD COLOMBIA LTDA y así poder reforzar e incluir nuevos controles, que permitan mitigar las vulnerabilidades existentes en la red interna de la empresa y así lograr proteger dichos activos de amenazas internas y/o externas, evitando perder información valiosa.

A continuación, se relacionan los criterios utilizados para realizar la valoración de la criticidad, impacto y riesgo, de los potenciales riesgos a los que se encuentran expuestos los activos de la información de la empresa CRAWFORD COLOMBIA LTDA.

9. EVALUACIÓN DEL RIESGO

DESCRIPCIÓN DE LA SITUACIÓN ACTUAL DE A LA SEGURIDAD DE LA INFORMACIÓN

De acuerdo a la Investigación de campo, la revisión bibliográfica y el enfoque exploratorio de la investigación cualitativa realizada a la empresa CRAWFORD COLOMBIA LTDA., se logra evidenciar que, en relación con la seguridad de la información la empresa presenta falencias ya que para acceder a ciertos recursos de información no se cuenta con parámetros establecidos que le restrinjan a los colaboradores el acceso ya que estos se encuentran alojados en la nube de Office 365 y en carpetas compartidas que se encuentran ubicadas en un servidor físico y para acceder a dichos activos de información solo es necesario que el usuario tenga un usuario dentro del dominio de red y una cuenta corporativa con el dominio de la empresa.

Respeto a la seguridad lógica de los cuatro servidores y la red de la empresa CRAWFORD COLOMBIA LTDA., la cual está conformada por cuarenta y cinco equipos y se encuentra configurada bajo una topología tipo estrella, se logra evidenciar que se comunican por medio de correos y los archivos se manejan por VPN, donde todos los equipos están conectados directamente a los Switches donde la empresa conecta al Router.

9.1. ALCANCE

Este análisis del riesgo de la información en CRAWFORD COLOMBIA LTDA busca encontrar las opciones de mejora en el manejo y la seguridad de la información, analizando cada uno de los activos de la empresa y el planteamiento de los interesados por que se tenga un adecuado manejo de la información y por medio de este análisis lograr evidenciar y mitigar los riesgos y afectaciones posibles a la información, mediante la implementación de listas de control de acceso (ACL) extendidas.

9.2. CONTEXTO

CRAWFORD COLOMBIA LTDA como una empresa ajustadora de seguros maneja información de alto valor de sus clientes que en este caso son las Aseguradoras, en donde se encuentra documentación de siniestralidades, pólizas, normatividad jurídica entre otros.

Teniendo en cuenta que la compañía utiliza toda esta información para hacer sus reportes o informes a las aseguradoras donde se denotan razones jurídicas o de procedimiento en donde una póliza puede cubrir o no un siniestro, sería demasiado grave para CRAWFORD COLOMBIA LTDA que toda esta información pueda ser filtrada, ya que compromete su capacidad de cumplimiento de acuerdos de confidencialidad con sus clientes.

Los factores, tanto internos como externos, son de gran importancia para el desarrollo de las actividades diarias en la empresa CRAWFORD COLOMBIA LTDA, por lo cual en la matriz DOFA, ver figura 10, se relacionan estos factores y se catalogan las fortalezas, debilidades, oportunidades y amenazas, adicionalmente se plantean las estrategias implementadas por la empresa.

Adicionalmente, para tener un contexto más claro, de los factores, internos y externos, que intervienen en la empresa, se utiliza la matriz PESTEL + Porter, ver figura 12, ya que en esta matriz se desglosan y se categorizan dichos factores.

Otro punto importante a tener en cuenta al momento de realizar el aseguramiento de los activos de información, son las partes interesas, ver figura 11, ya que estas partes contribuyen de manera relevante en la toma de decisiones y su participación, de una manera armónica, puede llegar a mejorar de manera relevante, el éxito del presente trabajo de investigación.

Figura 11. *Matriz DOFA*

DOFA		
FACTORES INTERNOS **FACTORES EXTERNOS**	**FORTALEZAS:** - La informacion esta almacenada en entronos de facil acceso para cualquier funcionario que la requiera. - La informacion cuenta con repaldos constantes en tiempo real y vesionamiento de archivos. - La empresa cuenta con una politica de seguridad de la infrmacion. - El departamento de Sistemas cuenta con personal capacitado para garantizar la seguridad de la informacion. - Interes por parte de la administarcion en el tratamiento de la informacion.	**DEBILIDADES:** -Los usuario finales tienen poco o ningun conocimiento en de losp recesos de las poslíticas de seguridad de la ifnromacion. - No hay controles de acceso a adicional para usuarios que se encuentren autenticados dentro de la red. -No hay claridad en las labores y por ende a que tipo de informacion deberia tener acceso o no cada departamento.
OPORTUNIDADES : - Establecer a cada uno de los actores de la empresa como partes importantes para la seguridad de la informacion. - Implementar una politica de acceso a la iformacion por medio de perfiles y permisos. - Capacitar a los usuarios en el manejo apropiado de la informacion.	**ESTRATEGIA F.O.** - Fortalecer el compromiso con la seguridad de la informacion por medio de capacitaciones constantes de metodos de mantener segura la informacion de la empresa y como ponemos en riesgo la informacion. - Capacitar constantemente al departamento de sistemas en el area de la seguridad informatica y nuevas amenazas. .	**ESTRATEGIAS D.O.** - Socializar a todos los involucrados con la informacion de la empresa las policitas de seguridad establecidas. - Desarrollar o actualzar mapa organizacional de la empresa para tener claridad de los roles y perfiles al momento de hacer la implementacion de una politica de acceso en la red.
AMENAZAS: - Filtracion de infmracion por falta de controles en los accesos. - Funcionarios consultan informacion por fuera sus horas de trabajo para fines no laborales. - Perdida de informacion o suplantacion por ataques ciberneticos. - Cambio de personal.	**ESTRATEGIAS F.A.** - Curso y capacitaciones para el personal de la empresa las buenas practicas del manejo de la informacion. - Creacion de dinamicas y campañas que fortalezcan la identidad corporativa.	**ESTRATEGIAS D.A**. - Hacer analisis de vulnerabiliadades del a informacion de la empresa periodicamente. - Creacion de departamento de riesgos de la informacion. - Destinar por lo menos a una persona al control de la seguridad de la informacion

Figura 11. Matriz DOFA

Fuente: Elaboración propia 2021 (Crawford Colombia, 2020)

Figura 12. *Matriz Poder-Interés*

PODER		INTERES	
		BAJO	ALTO
ALTO		SATISFACER VS-001, VS-006, VS-007, VS-009	COLABORAR VS-005, VS-010, VS-011
BAJO		OBSERVAR VS-003, VS-013	COMUNICAR VS-002, VS-004, VS-008, VS-012, VS-014, VS-015

Cod.	Stakeholders
VS-001	Clientes y asegurados
VS-002	Medios de comunicación
VS-003	Sociedad
VS-004	Proveedores
VS-005	Empleados
VS-006	Organismos reguladores y supervisores
VS-007	Accionistas, inversores y socios
VS-008	colaboradores
VS-009	Organismos reguladores y supervisores
VS-010	Junta directiva
VS-011	Directores de proyecto
VS-012	Área de contavilidad
VS-013	Área de RRHH
VS-014	Departamento de compras
VS-015	Coordinación de proveedores

Figura 12. Matriz Poder-Interés

Fuente: Elaboración propia 2021 (Crawford Colombia, 2020)

Figura 13. *Matriz PESTEL + Porter*

Figura 13. Matriz PESTEL + Porter

Fuente: Elaboración propia 2021 (Crawford Colombia, 2020)

9.3. CRITERIOS

Para lograr obtener una estimación adecuada del riesgo, es necesario dar claridad a qué corresponde cada valor de probabilidad e impacto que se le dará a cada riesgo.

Probabilidad

En la figura 13, se relacionan la probabilidad de ocurrencia de eventos de riesgo en la seguridad de la información, este criterio se logra determinar mediante el análisis de la matriz de riesgos, ver figura 17, teniendo en cuenta la valoración de activos de seguridad, ver figura 15 y de acuerdo a las necesidades del negocio indicadas y determinadas por la empresa CRAWFORD COLOMBIA LTDA.

Figura 14. *Cuadro Probabilidad*

PROBABILIDAD	
Casi Seguro	Evento que puede ocurrir en la mayoría de circunstancias mas de 15 veces en un año
Probable	Evento que ocurre casi siempre entre 11 y 15 veces al año
Posible	Evento que ocurre en algunas circunstancias entre 6 y 10 veces al año
Improbable	Evento que puede ocurrir en pocas circunstancias entre 2 y 5 veces al año
Raro	Puede ocurrir en circunstancias excepcionales

Figura 14. Cuadro Probabilidad

Fuente: Elaboración propia 2021

Impacto

En la figura 14, se relacionan el impacto que podría llegar a tener la ocurrencia de eventos de riesgo en la seguridad de la información, este criterio se logra determinar mediante el análisis de la matriz de riesgos, ver anexo 2, y teniendo en cuenta la valoración de activos, ver anexo 1, el cuadro de probabilidad, ver figura 13, la posición en el mapa de calor, ver figura 15 y de acuerdo a las necesidades del negocio indicadas y determinadas por la empresa CRAWFORD COLOMBIA LTDA.

Figura 15. *Cuadro Impacto*

IMPACTO	
Catastrófico	Imagen corporativa a nivel nacional e Internacional afectada ,al igual que la operación por el incumplimiento en sus deberes corporativos, filtración de documentación delicada de sus clientes en el manejo de siniestros
Mayor	Imagen corporativa a nivel nacional afectada, al igual que la operación por el incumplimiento en sus deberes corporativos
Moderado	Afecta negativamente la imagen dela empresa en sus clientes por retrasos en la prestación delos servicios
Menor	Impacta negativamente la operación dela empresa, se pueden presentar retrasos en la operación y sobrecostos por reprocesos
Insignificante	Impacta negativamente de forma leve la imagen y operación de la empresa. No tiene Impacto relevante en la Información o sus procesos

Figura 15. Cuadro Impacto

Fuente: Elaboración propia 2021

Se estableció el nivel de riesgo de acuerdo a la combinación de probabilidad e impacto según el mapa de calor, ver figura 15, en la cual se realizan combinaciones de riesgo, en donde rojo es extremo, naranja es alto, amarillo es moderado y verde es bajo. También se hizo una ponderación de porcentaje de afectación del riesgo los cuales al acercarse a un 100% en la combinación de probabilidad / impacto representa un riego grande para CRAWFORD COLOMBIA LTDA.

Para la compañía, la seguridad de su información representa la credibilidad y confianza depositada por sus clientes (Aseguradoras), por eso ningún riesgo en la cuarta (4) o quinta (5) escala del mapa de calor podrá ser tolerado y se deberán tomar medidas que mitiguen estos valores.

Figura 16. *Posiciones en el mapa de calor*

			IMPACTO				
			Insignificante	Menor	Moderado	Mayor	Catastrófico
			1	2	3	4	5
PROBABILIDAD	Casi Seguro	5	A	A	E	E	E
	Probable	4	M	A	A	E	E
	Posible	3	B	M	A	E	E
	Improbable	2	B	B	M	A	E
	Raro	1	B	B	M	A	A

Figura 16. Posiciones en el mapa de calor

Fuente: Elaboración propia 2021

La valoración de activos, ver anexo 1, se realiza mediante los criterios indicados y determinados por la empresa CRAWFORD COLOMBIA LTDA, en la cual se da una calificación comprendida entre uno y cinco, ver figura 16, a cada uno de los activos de información, esta calificación se realiza teniendo en cuenta la afectación que puedan llegar a tener cada uno de los pilares de la seguridad de la información (confidencialidad, integridad y disponibilidad), al verse vulnerados, adicionalmente se tiene en cuenta la importancia que representa cada uno de estos activos para la empresa, esta calificación se encuentra comprendida entre uno y cinco, lo cual arroja una valoración total del activo, lo cual brinda un criterio para asegurar el activo, mediante la elevación o denegación de los permisos de usuario.

La matriz de riesgos, ver anexo 2, se desarrolla teniendo en cuenta los criterios indicados y determinados por la empresa CRAWFORD COLOMBIA LTDA, para lograr determinar criticidad del impacto en la ocurrencia de eventos de riesgo en la seguridad de la información, estos riesgos deben clasificarse de acuerdo con los parámetros establecidos en el cuadro de probabilidad, ver figura 13, y el cuadro de impacto, ver figura 14.

9.4. VALORACIÓN DE ACTIVOS EN LA EMPRESA CRAWFORD COLOMBIA LTDA (VER ANEXO 1)

En la presente matriz se relacionan los activos de información definidos por la empresa CRAWFORD COLOMBIA LTDA, en los cuales se pretende establecer los beneficios de la aplicación de las listas de control de acceso (ACL) y las restricciones a los permisos de los usuarios para acceder a ciertos archivos para reducir las vulnerabilidades en el manejo de la información y la carga de la red.

ANEXO 1.pdf

9.5. MATRIZ DE RIESGOS EN LA EMPRESA CRAWFORD COLOMBIA LTDA (VER ANEXO 2)

En la presente matriz se relacionan los eventos de riesgo en la seguridad de la información identificados por la empresa CRAWFORD COLOMBIA LTDA.

ANEXO 2.pdf

Figura 17. *Escala de valoración de activos*

Valoración de Activos	
5	Critico
4	Alto
3	Medio
2	Bajo
1	Mínimo

Figura 17. Escala de valoración de activos

Fuente: Elaboración propia 2021

9.6. RIESGO INHERENTE

De acuerdo con la información que se refleja en el matriz de riesgos, ver anexo 2, y en la valoración de activos, ver anexo 1, y de acuerdo con los controles, que tiene implementados la empresa CRAWFORD COLOMBIA LTDA, ver anexo 3, se logra determinar el mapa de calor de riesgo inherente, ver figura 17, en el cual se logran evidenciar los activos de información que se encuentran con mayor probabilidad de ocurrencia de un evento de riesgo en la seguridad de la información.

Figura 18. *Mapa de calor riesgo inherente en la empresa CRAWFORD COLOMBIA LTDA*

MAPA DE CALOR RIESGO INHERENTE

PROBABILIDAD		IMPACTO				
		Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
Casi Seguro	5					
Probable	4	Riesgo_44 -	Riesgo_72 -	Riesgo_20 - Riesgo_22 - Riesgo_47 -	Riesgo_21 - Riesgo_23 - Riesgo_46 - Riesgo_51 -	Riesgo_70 - Riesgo_74 -
Posible	3		Riesgo_3 - Riesgo_4 - Riesgo_36 - Riesgo_39 -	Riesgo_1 - Riesgo_2 - Riesgo_5 - Riesgo_6 -	Riesgo_15 - Riesgo_16 - Riesgo_38 - Riesgo_40 -	
Improbable	2	Riesgo_32 - Riesgo_48 -	Riesgo_10 - Riesgo_11 - Riesgo_13 - Riesgo_17 -	Riesgo_19 - Riesgo_67 -		
Raro	1	Riesgo_12 -	Riesgo_33 -	-		

Figura 18. Mapa de calor riesgo inherente en la empresa CRAWFORD COLOMBIA LTDA

Fuente: Elaboración propia 2021

Teniendo en cuenta la información registrada en el mapa de calor del riesgo inherente de la empresa CRAWFORD COLOMBIA LTDA, ver figura 17, y los controles implementados por empresa, más la configuración de las listas de control de acceso (ACL) extendidas en el router que conecta los a las áreas de la empresa, ver anexo 3, se fomenta la separación de privilegios, definiendo los permisos de acceso a un determinado objeto, permitiendo ejercer un control eficaz al flujo del tráfico en equipos de red (terminales de trabajo), así como a los swithes y el router. Estas políticas se evalúan de acuerdo al orden en que fueron introducidas en la ACL, al momento en el que los paquetes llegan a la interfaz del router, se hace la comparación uno a uno y en secuencia, instrucción por instrucción hasta encontrar una coincidencia, una vez detectada las coincidencias, se ejecuta la acción específica en la sentencia y no se comprueban más condiciones, adicionalmente mediante la implementación del principio del mínimo privilegio (PoLP), se logra establecer que, con estos controles adicionales, la probabilidad de ocurrencia de un evento de riesgo en la seguridad de la información se ve disminuido, ya que los activos de información que se encuentran con una probabilidad de ocurrencia posible y/o probable, con un impacto mayor y/o catastrófico, salen de estas área de riesgo y se ubican en una posición más segura, lo cual se visualiza de manera más clara en el mapa de calor del riesgo residual, ver figura 18.

9.7. MATRIZ DE CONTROLES EN LA EMPRESA CRAWFORD COLOMBIA LTDA (VER ANEXO 3)

En la presente matriz se relacionan los controles existentes en la empresa CRAWFORD COLOMBIA LTDA y se adicionan los controles sugeridos en el presente trabajo de investigación mostrando el riesgo residual con la aplicación de las listas de control de acceso (ACL) y el principio de mínimo privilegio en la asignación de roles de usuarios.

ANEXO 3.pdf

Figura 19. *Mapa de calor riesgo residual en la empresa CRAWFORD COLOMBIA LTDA*

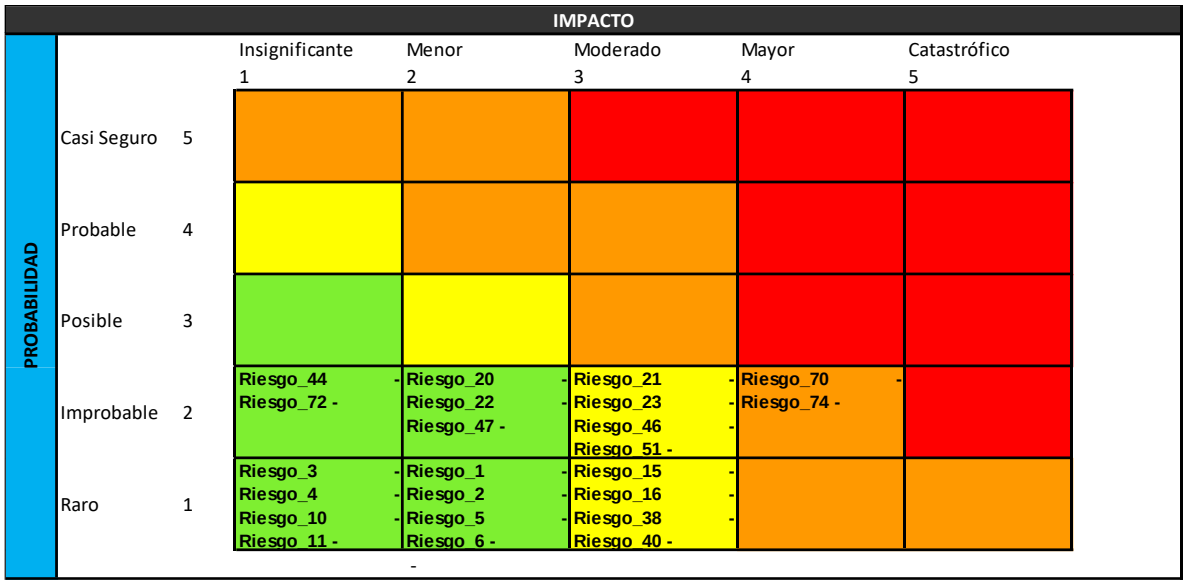

Figura 19. Mapa de calor riesgo residual en la empresa CRAWFORD COLOMBIA LTDA

Fuente: Elaboración propia 2021

10. DEFINICIÓN DE LAS LISTAS DE CONTROL DE ACCESO (ACL) EXTENDIDAS EN LA EMPRESA CRAWFORD COLOMBIA LTDA

Figura 20. *Protocolos y números de puertos a configurar*

Puerto/Protocolo	Nombre	Descripción
25/TCP	SMTP	Transferencia de correo electrónico vía Internet
110/TCP	POP3	Transferencia de correo electrónico corporativo
20/TCP	FTPS-data	Control de transferencia de archivos
23/TCP	Telnet	Control remoto de equipos
443/TCP	HTTPS	Transferencia segura de paginas web
445/TCP	Microsoft-ds	Tráfico compartido de archivos e impresoras

Figura 20. Protocolos y números de puertos a configurar

Fuente: Elaboración propia 2021

La empresa CRAWFORD COLOMBIA LTDA, al contar con una topología tipo estrella, permite realizar un enfoque detallado a la seguridad de los switches que conectan al router, el cual realiza la conexión de cada área de la empresa con el servidor de archivos, el servidor de correo corporativo y el servidor web, ubicados en el data center de la empresa, donde reposan las activos de información, que de acuerdo con las necesidades del negocio, son de vital importancia para el normal desarrollo de las actividades diarias de la empresa.

Se debe tener en consideración que mediante la implementación de las listas de control de acceso (ACL) extendidas, se puede ejercer un mejor control, ya que estas son más específicas, la permitir realizar el filtrado, por tipo de tráfico que viaja a través de la red, adicionalmente, permite filtrar las direcciones IP, números de puerto de origen y destino, ya que son requisitos establecidos en la sintaxis de las listas, realizar la especificación de un protocolo y la condición de permitir o denegar, un ejemplo puede ser, un protocolo IP, indicar todo el tráfico IP, o puede indicar el filtrado en un protocolo IP específico, como TCP, UDP, ICMP y OSPF, este tipo de filtrado se realiza mediante el análisis de los paquetes entrantes y salientes, y la transferencia o el bloqueo de estos según criterios determinados al momento de establecer las ACL, es importante mencionar que las listas de control de acceso (ACL) extendidas, permiten filtrar los paquetes que viajan por las capas 3 y 4 (red y transporte) del modelo OSI.

De acuerdo a la observación realizada a la arquitectura de red de la empresa, el análisis realizado a las matrices utilizadas a lo largo del desarrollo del presente trabajo de investigación y requerimientos del negocio, se lograron definir las siguientes listas de control de acceso (ACL) extendidas.

Todos los puertos del router de la empresa se configuran para que se encuentren en estado apagado.

Desde el switch (SW1) asignado al Departamento Sistemas, se le permitirá al director del departamento, o quien haga sus veces, el tráfico Telnet, el tráfico ICMP, el tráfico SMTP, el tráfico POP3, el tráfico HTTPS a las direcciones IP que no se encuentren en lista negra, el tráfico SMB y el tráfico FTPS, los demás equipos de cómputo asignados al departamento

solo tendrán acceso a tráfico POP3, FTPS, SMB y HTTPS a la dirección IP de la intranet de la empresa, el tráfico restante queda bloqueado.

El director del departamento de sistemas, o quien haga sus veces, determinara cuales de sus colaboradores deben tener habilitado el tráfico Telnet, teniendo en cuenta que, este tráfico solo debe ser utilizado para realizar el soporte remoto y el tráfico ICMP teniendo en cuenta que, este tráfico solo debe ser utilizado para lograr detectar posibles errores en los servicios de red, los tráficos mencionados con anterioridad, se deben realizar de acuerdo a las políticas de seguridad de la información establecidas por la empresa y previa autorización del director de departamento de sistemas o quien haga sus veces.

Teniendo en cuenta que cada una de las áreas de la empresa CRAWFORD COLOMBIA LTDA tiene asignado un número de equipos de cómputo y los colaboradores asociados a dichas áreas tiene asignado a su inventario personal un equipo, permite configurar en dichas terminales las listas de control de acceso (ACL) extendidas, para asignar los permisos correspondientes para el acceso a los activos de información.

Desde el switch (SW2) asignado a la gerencia general y gerencia administrativa, se permite el tráfico SMTP, tráfico POP3, tráfico HTTPS, el tráfico SMB y tráfico FTPS total a cualquier destino de la red (Departamento Sistemas / Departamento Gestión Documental / Departamento Cartera / Departamento Financiero / Dirección de Operaciones), servidor de aplicación, servidor de correo corporativo y servidor web.

Desde el switch (SW3) asignado al Departamento Gestión Documental, se le permitirá al director del departamento, o quien haga sus veces, el tráfico Telnet, el tráfico ICMP, el tráfico SMTP, el tráfico POP3, el tráfico HTTPS a las direcciones IP que no se encuentren en lista negra, el tráfico SMB y el tráfico FTPS, los demás equipos de cómputo asignados al departamento solo tendrán acceso a tráfico POP3, FTPS, SMB y HTTPS a la dirección IP de la intranet de la empresa, el tráfico restante queda bloqueado.

Desde el switch (SW4) asignado al Departamento Cartera, se le permitirá al director del departamento, o quien haga sus veces, el tráfico Telnet, el tráfico ICMP, el tráfico SMTP, el tráfico POP3, el tráfico HTTPS a las direcciones IP que no se encuentren en lista negra, el tráfico SMB y el tráfico FTPS, los demás equipos de cómputo asignados al departamento solo tendrán acceso a tráfico POP3, FTPS, SMB y HTTPS a la dirección IP de la intranet de la empresa, el tráfico restante queda bloqueado.

Desde el switch (SW5) asignado al Departamento Financiero, se le permitirá al director del departamento, o quien haga sus veces, el tráfico Telnet, el tráfico ICMP, el tráfico SMTP, el tráfico POP3, el tráfico HTTPS a las direcciones IP que no se encuentren en lista negra, el tráfico SMB y el tráfico FTPS, los demás equipos de cómputo asignados al departamento solo tendrán acceso a tráfico POP3, FTPS, SMB y HTTPS a la dirección IP de la intranet de la empresa, el tráfico restante queda bloqueado.

Desde el switch (SW6) asignado al Dirección de Operaciones, se le permitirá al director del departamento, o quien haga sus veces, el tráfico Telnet, el tráfico ICMP, el tráfico SMTP, el tráfico POP3, el tráfico HTTPS a las direcciones IP que no se encuentren en lista negra, el tráfico SMB y el tráfico FTPS, los demás equipos de cómputo asignados al departamento

solo tendrán acceso a tráfico POP3, FTPS, SMB y HTTPS a la dirección IP de la intranet de la empresa, el tráfico restante queda bloqueado.

De acuerdo con los manuales de funciones y las políticas de seguridad de la información, se determinará a cuáles colaboradores de las áreas de la empresa es necesario habilitarles otro tipo de tráfico, diferente al establecido en las presentes listas de control de acceso (ACL) extendidas, esta solicitud se debe realizar por medio del director de departamento correspondiente o quien haga sus veces.

Las listas de control de acceso (ACL) extendidas, sugeridas permiten que se limite el tráfico de la red para aumentar la seguridad y el rendimiento de la misma, al filtrar el tráfico de acuerdo al tipo, permitiendo que las diferentes áreas de la CRAWFORD COLOMBIA LTDA, solo puedan generar tráfico TCP/IP al servidor de archivos, tráfico de correo electrónico corporativo y tráfico a la intranet corporativa, el tráfico restante, si no es necesario para desarrollar las actividades diarias de la compañía, queda bloqueado.

Para regular el acceso a los activos de información almacenados en el servidor de archivos ubicado en el data center de la empresa, y de acuerdo con las políticas PoLP, se sugiere que los permisos de acceso sean establecidos inicialmente como consulta, y de acuerdo con los manuales de funciones y las políticas de seguridad de la información se escalen los respectivos permisos elevándolos a administrador, lectura, escritura modificación, eliminación y/o el rol excepcional el cual agrupa todos los permisos, esta solicitud se debe realizar por medio del director de departamento correspondiente o quien haga sus veces.

Teniendo en cuenta la información arrojada mapa de calor del riesgo residual, ver figura 19, se logra evidenciar los beneficios de la aplicación de las listas de control de acceso (ACL) y las restricciones a los permisos de los usuarios para acceder a ciertos archivos para reducir las vulnerabilidades en el manejo de la información y la carga de la red en la empresa CRAWFORD COLOMBIA LTDA, ya que los activos información que se encuentran con una probabilidad de ocurrencia posible y/o probable, con un impacto mayor y/o catastrófico, salen de estas área de riesgo y se ubican en una posición más segura.

11. RECOMENDACIONES

A la par de la implementación de las listas de control de acceso (ACL) para lograr mejora la seguridad de la información en la Empresa CRAWFORD COLOMBIA LTDA, se recomienda realizar ciclos de capacitaciones, de manera continua, que se encuentren enfocadas en la seguridad de la información y mejora continua.

El inventario e identificación de los activos de información deben ser actualizados de manera continua, de acuerdo con las necesidades del negocio.

Exigir que el usuario se autentique con su cuenta y usuario de dominio del directorio activo antes de crear una sesión puede llegar a mejora la seguridad del servidor de Host de sesión, al solicitar una autenticación a nivel de red.

El implementar una política de gestión de contraseñas en el directorio activo, lo cual ayudara a garantizar que cumplan con el nivel requerido y se apliquen de manera consistente.

Mediante la utilización en forma estricta de la regla del mínimo privilegio por parte del directorio activo, en la asignación y el uso de los derechos de acceso privilegiado, se controla el acceso y las posibles modificaciones a los activos de información.

Es de gran utilidad utilizar de manera periódica la suplantación de identidad vía IP (IP spoofing) de manera controlada, para verificar la seguridad de la red de la empresa, ya que al hacer uso de un direccionamiento IP, un ciberdelincuente se puede suplantar a un usuario de la red de la empresa y así lograr conocer sus datos de acceso.

Teniendo en cuenta que las listas de control de acceso (ACL) cuentan con una sintaxis básica de configuración, se recomienda consultar dicha sintaxis en la figura 21.

Figura 21. *Configuración de listas de control de acceso (ACL) Extendidas*

access-list-number	Identifica las listas de acceso con un número de rango entre 100 y 199 (para una ACL IP extendida) y entre 2000 y 2699 (para una ACL IP expandida).
deny	Deniega el acceso si las condiciones concuerdan.
permit	Permite el acceso si las condiciones concuerdan.
remark text	Se utiliza para introducir comentarios.
protocol	Nombre o número un protocolo de internet. Algunas de las palabras clave más comunes son icpm, ip, tcp, o udp. Para que haya coincidencias con cualquier protocolo de internet (como ICPM, TCP y UDP), se usa la palabra clave ip.
origen	Número de la red o del host desde el que se envía el paquete.
source	Identifica la red de origen o la dirección de host que se va a filtrar. Algunos de los operadores posibles son: any (para especificar todas las redes), host ip-address (para identificar una dirección IP específica).
source-wildcard	Bits de wildcard para aplicar al origen.
destination	Identifica la red de destino o la dirección de host que se va a filtrar. Algunos de los operadores posibles son: any (para especificar todas las redes), host ip-address (para identificar una dirección IP específica).
destination-wildcard	Bits de wildcard para aplicar al destino.
operator	(Opcional) Compara los puertos de origen y destino. Algunos de los operadores posibles son: lt (menor que), gt (mayor que), eq (igual a), neq (distinto de), and range (rango inclusivo).
puerto	(Opcional) El número decimal o nombre de un puerto TCP o UDP.
established	(Opcional) Solo para el protocolo TCP: indica una conexión establecida.

Figura 21. Configuración de listas de control de acceso (ACL) Extendidas

Fuente: Configuración de ACL de IPV4 Extendidas (ITESA, s.f)

Cada entrada de una ACL incluye el uso de una máscara wildcard, la cual es una cadena de 32 dígitos binarios que el router utiliza para determinar qué bits de la dirección del paquete debe examinar para obtener una coincidencia.

Implementar listas de control de acceso (ACL) extendidas, ya que estas proporcionan un mayor grado de control, teniendo en cuenta que, mediante estas políticas, se puede filtrar por dirección de origen, dirección de destino, protocolo (IP, TCP, UDP, ICMP) y número de puerto.

Mediante las listas de control de acceso (ACL) extendidas, se puede permitir el tráfico de correo electrónico de una red a un destino específico y, simultáneamente, denegar la transferencia de archivos y la navegación web.

Las listas de control de acceso (ACL) extendidas usan un número de access-list que va de 100 a 199 y de 2000 a 2699.

Las listas de control de acceso (ACL) extendidas se deben establecer cerca de la fuente de tráfico de datos, para bloquear el tráfico de datos desde el origen al destino, se recomienda aplicar una ACL entrante al puerto E0 en el router A en vez de una lista saliente al puerto E1 en el router B.

Separar el tráfico mediante VLANs, para que la red quede acotada a un único segmento lógico.

Las listas de control de acceso (ACL) extendidas permiten trabajar al nivel de las capas 3 y 4, capa de red y capa de transporte, del modelo OSI, y esto permite que sean los propios equipos de red los que permitan o denieguen cierto tipo de comunicaciones antes de llegar a los firewalls.

Tener una lista de acceso por protocolo, por dirección y por interfaz.

Tener una lista de acceso de entrada y una de salida aplicada a una interfaz.

No tener dos listas de acceso a la dirección entrante de una interfaz.

12. CONCLUSIONES

Idealmente, habría un sistema de calificación de riesgo universal que calcularía con precisión todos los riesgos para todas las organizaciones. Pero una vulnerabilidad que es crítica para una organización puede no ser muy importante para otra. Entonces, se presenta un marco básico que debe personalizarse para la organización en particular.

Para mejorar la organización de tráfico de datos y seguridad de la información de la empresa CRAWFORD COLOMBIA LTDA, se debe examinar la implementación de las listas de control de acceso (ACL) extendidas como una necesidad esencial en el manejo de flujo de datos de la empresa, debido a que es una herramienta que ayuda a identificar los posibles riesgos informáticos a los que puedan estar enfrentados.

Se deben definir de manera correcta los requerimientos de seguridad de la red y los roles y permisos de los usuarios, para que de esta manera las políticas de seguridad respondan de forma correcta a las necesidades de la misma.

Las políticas de seguridad deben ser lo más clara y específicamente escritas para que todos los colaboradores sin excepción alguna, las entiendan de forma inmediata y no den cabida a una segunda interpretación. Estas políticas no solo tienen la función de fijar un reglamento para que los empleados sigan, sino que, además, estas deben concientizar a los empleados sobre los riesgos y la importancia de acatarlas al pie de la letra.

Las políticas creadas deben ser implementadas en un servidor que cuente con un servicio proxy, el cual es muy recomendable utilizar en una empresa para filtrar y crear restricciones hacia los sitios de internet a los cuales se pueden conectar los usuarios y puedan alterar la seguridad. Sin embargo, este debe ser lo suficientemente eficiente para que no genere cuellos de botella y haga que la red funcione de forma lenta.

La seguridad en puerto y un NAC (Network Access Control) son otras de las medidas a tener en cuenta.

13. BIBLIOGRAFÍA

Álvarez Marañón, G., & Pérez García, P. P. (2004). *Seguridad informática para empresas y particulares.* Madrid, España: Mc Graw Hill. Recuperado el 11 de 02 de 2021, de https://online.fliphtml5.com/oazu/cgdk/#p=50

Barceló Ordinas, J. M., Íñigo Griera, J., Martí Escalé, R., Peig Olivé, E., & Perramon Tornil, X. (2004). Recuperado el 10 de 02 de 2021, de https://libros.metabiblioteca.org/bitstream/001/341/9/84-9788-117-6.pdf

Berenguer Serrato, D. (06 de 2018). Recuperado el 12 de 02 de 2021, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

Cancillería de Colombia. (17 de 03 de 2020). Recuperado el 26 de 02 de 2021, de https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

Cano M., J., & Almanza, A. (02 de 03 de 2020). Recuperado el 31 de 05 de 2021, de https://www.researchgate.net/project/Encuesta-Colombiana-de-Seguridad-Informatica

Carvajal, A. (2013). Obtenido de https://www.globalteksecurity.com/docs/book/INSEGURIDAD_DE_LA_INFORMACION.pdf

Cisco. (27 de 12 de 2007). *Cisco*. Obtenido de Configuración de listas de Acceso IP: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

Cisco. (13 de 12 de 2018). Recuperado el 16 de 02 de 2021, de https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-350-series-managed-switches/smb3050-configure-ipv6-based-access-control-list-acl-and-access-cont.html

Congreso de la República de Colombia. (31 de 12 de 2008). Obtenido de http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf

Congreso de la República de Colombia. (05 de 01 de 2009). Obtenido de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Congreso de la República de Colombia. (15 de 07 de 2009). Recuperado el 18 de 02 de 2021, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=36841

Congreso de la República de Colombia. (17 de 10 de 2012). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Consejo Nacional de Política Económica y Social. (14 de 06 de 2011). Recuperado el 26 de 02 de 2021, de https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

Crawford Colombia. (16 de 03 de 2020). Recuperado el 15 de 04 de 2021, de https://www.crawfordcolombia.com/

Cyberark. (s.f.). Recuperado el 11 de 02 de 2021, de https://www.cyberark.com/es/what-is/least-privilege/

Cybereop. (s.f). Recuperado el 24 de 02 de 2021, de https://www.cybereop.com/blog/te-presentamos-nuestra-revista-ciberseguridad-pyme.html

CyberSecurity. (02 de 06 de 2019). Recuperado el 26 de 02 de 2021, de https://hard2bit.com/blog/como-ha-evolucionado-la-ciberseguridad-en-los-ultimos-25-anos-y-como-ha-sido-la-evolucion-de-seguridad-en-las-empresas/

Docplayer. (01 de 04 de 2020). Recuperado el 27 de 02 de 2021, de http://docplayer.es/186386951-Lista-de-control-de-acceso-acl-y-entrada-de-control-de-acceso-ace-de-la-configuracion-ipv6-based-en-un-switch.html

Europapress. (24 de 11 de 2017). Recuperado el 23 de 02 de 2021, de https://www.europapress.es/portaltic/ciberseguridad/noticia-peor-vulnerabilidad-contra-ciberseguridad-empresas-usuario-20171124140136.html

Figueroa Suárez, J., Rodríguez Andrade, R., Bone Obando, C., & Saltos Gómez, J. (15 de 12 de 2017). Recuperado el 31 de 05 de 2021, de https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf

Hernandez, T., Salazar, P., & Soto, S. (28 de 08 de 2017). Recuperado el 31 de 05 de 2021, de https://www.ecorfan.org/taiwan/research_journals/Simulacion_Computacional/vol1num2/Revista_de_Simulaci%C3%B3n_Computacional_V1_N2.pdf#page=31

ICONTEC. (22 de 03 de 2006). Recuperado el 10 de 02 de 2021, de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

ICONTEC. (22 de 03 de 2006). Recuperado el 26 de 02 de 2021, de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

ICONTEC. (2008). Recuperado el 25 de 02 de 2021, de http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107

ICONTEC. (2 de 12 de 2020). *Normas Icontec.* Recuperado el 30 de 01 de 2021, de https://concepto.de/teoria-del-big-bang/#ixzz6l318Yi1r

INCIBE. (27 de 03 de 2017). Recuperado el 26 de 02 de 2021, de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

ISOTools. (06 de 08 de 2015). Recuperado el 25 de 02 de 2021, de https://www.isotools.org/2015/08/06/en-que-consiste-una-matriz-de-riesgos/

ITESA. (s.f). Recuperado el 10 de 04 de 2021, de https://www.itesa.edu.mx/netacad/switching/course/module9/9.3.2.1/9.3.2.1.html

Kaspersky. (s.f). Recuperado el 23 de 02 de 2021, de https://latam.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

Knipp, E., Browne, B., Weaver, W., Baumrucker, C. T., Chaffin, L., Caesar, J., & Osipov, V. (2000). *Managing Cisco Network Security.* (E. Danielyan, Ed., & H. A. Moreno Duarte, Trad.) SYNGRESS. Recuperado el 12 de 02 de 2021, de https://www.elsevier.com/books/managing-cisco-network-security/syngress/978-1-931836-56-2

Mifsud, E. (30 de 09 de 2012). Recuperado el 06 de 02 de 2021, de http://recursostic.educacion.es/observatorio/web/gl/software/servidores/1065-listas-de-control-de-acceso-acl?start=3

Montoya S., J., & Restrepo R., Z. (09 de 04 de 2012). Recuperado el 06 de 02 de 2021, de https://dialnet.unirioja.es/descarga/articulo/4694078.pdf

Oracle Corporation. (2002, 2011). Recuperado el 12 de 02 de 2021, de https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html

Organización de los Estados Americanos. (2018). Recuperado el 11 de 02 de 2021, de https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

OWASP. (2017). Recuperado el 01 de 03 de 2017, de https://owasp.org/www-pdf-archive/OWASP-Top-10-2017-es.pdf

Peña, L. (2010). Recuperado el 04 de 06 de 2021, de https://anestesiar.org/guia-para-autores/autores-revision-bibliografica/

Pita Fernández, S., & Pértegas Díaz, S. (27 de 05 de 2002). Recuperado el 26 de 02 de 2021, de https://www.fisterra.com/mbe/investiga/cuanti_cuali/cuanti_cuali2.pdf

Rincón, W. A. (2014). Administración de políticas de seguridad en una red de datos bajo una estructura de red definida a través de la utilización del servidor pfense. *Universidad Santo Tomás*, 13.

RISCE Revista Internacional de Sistemas Computacionales y Electrónicos. (11 de 2011). Recuperado el 10 de 02 de 2021, de https://www.uaeh.edu.mx/investigacion/icbi/LI_FisMat/itza_ortiz/RISCENoviembre2011.pdf

Rojas, J. A. (2011). Sistemas Detectores de Intrusos y Análisis de Funcionamiento del Proyecto de Código Abierto Snort. *Redes de Ingeniería* , 103-104.

Trivoli Software. (1 de Enero de 2006). Obtenido de publib.boulder: http://publib.boulder.ibm.com/tividd/td/ITAME/GC23-4684-00/es_ES/HTML/adminmst06.htm

ANEXO 1 - VALORACIÓN DE ACTIVOS EN LA EMPRESA CRAWFORD COLOMBIA LTDA.

Nombre del Activo	Descripción	Tipo de Activo	Confidencialidad	Integridad	Disponibilidad	Valor Corporativo del Activo	Valoración	Nivel de Clasificacion	Soporte	Ubicacion		Propietario	Responsable	Custodio
										Fisico	Electrónico			
Documentos Dirección empresarial	Documentación corporativa de Crawford Colombia	Información	4	3	2	4	4	Confidencial	Digital		Presidencia / Direccion empresarial	Gerencia General	Presidente	Departamento TI
Documentos Junta Directiva	Actas de reuniones, Contratos accionistas	Información	3	2	2	3	3	Privada	Digital		Presidencia / Junta Directiva	Gerencia General	Gerente General	Departamento TI
Facturas emitidas a clientes internacionales	Facturas pendientes por pagar de clientes internacionales	Información	4	3	3	4	4	Confidencial	Digital		Gerencia Administrativa / Cartera / Clientes Internacionales	Gerencia Administrativa	Recaudador	Departamento TI
Facturas emitidas a clientes nacionales	Facturas pendientes por pagar de clientes nacionales	Información	4	3	3	4	4	Confidencial	Digital		Gerencia Administrativa / Cartera / Clientes nacionales	Gerencia Administrativa	Recaudador	Departamento TI
Informes des gestión de Cartera	Informes de gestión de cobranza y seguimiento de cartera	Información	2	2	1	3	2	Privada	Digital		Gerencia Administrativa / Cartera / Informes	Cartera	Recaudador	Departamento TI
Certificados de retención proveedores	Certificados de pagos a proveedores	Información	4	4	3	3	3	Privada	Digital		Gerencia Administrativa/ Contabilidad / Certifiacados Retencion	Contabilidad	Contador	Departamento TI
Base de datos proveedores	Lista de proveedores Crawford con información de contactos	Información	3	3	4	3	3	Privada	Digital		Gerencia Administrativa / Contabilidad / Proveedores	Contabilidad	Contador	Departamento TI
Rut proveedores	Documentación de ubicación y clasificación de proveedores	Información	3	3	4	3	3	Privada	Digital		Gerencia Administrativa / Contabilidad / Proveedores	Contabilidad	Contador	Departamento TI
Documentos Nomina	Información de pagos a funcionarios vinculados directamente con Crawford Colombia	Información	4	5	5	5	5	Confidencial	Digital		Gerencia Administrativa / Contabilidad / Nomina	Contabilidad	Contador	Departamento TI
Pagos Seguridad Social	Certificados de pagos seguridad social	Información	3	2	3	3	3	Privada	Digital		Gerencia Administrativa / Contabilidad / Seguridad Social	Contabilidad	Contador	Departamento TI
Estados Financieros	Informes financieros o estados contables	Información	4	4	3	4	4	Privada	Digital		Gerencia Administrativa / Gerencia Administrativa / Contabilidad / Estados	Contabilidad	Contador	Departamento TI
Facturas a desarrollar clientes nacionales	Facturas emitidas a aseguradoras o reaseguradoras nacionales	Información	3	4	3	4	4	Confidencial	Digital		Gerencia Administrativa / Gerencia Administrativa / Contabilidad /	Contabilidad	Contador	Departamento TI
facturas desarrolladas clientes internacionales	Facturas emitidas a aseguradoras o reaseguradoras internacionales	Información	3	4	3	4	4	Confidencial	Digital		Gerencia Administrativa / Gerencia Administrativa / Contabilidad /	Contabilidad	Contador	Departamento TI
Formatos departamento contable	formatos de solicitudes y comunicaciones	Información	3	2	3	2	2	Privada	Digital		Gerencia Administrativa / Gerencia Administrativa / Contabilidad /	Contabilidad	Contador	Departamento TI
Implementación Factura electrónica	Documentación de capacitaciones, reuniones y procesos de facturación electrónica	Información	2	2	2	3	3	Privada	Digital		Gerencia Administrativa / Gerencia Administrativa / Contabilidad /	Contabilidad	Contador	Departamento TI
Monetizaciones	Certificaciones bancarias de cambios de divisas	Información	4	3	3	4	4	Confidencial	Digital		Gerencia Administrativa / Gerencia Administrativa / Contabilidad /	Contabilidad	Contador	Departamento TI
Presupuestos	Presupuestos anuales de Crawford Colombia	Información	3	4	3	3	3	Privada	Digital		Gerencia Administrativa / Gerencia Administrativa / Contabilidad /	Contabilidad	Contador	Departamento TI
Informes de facturación	Informes mensuales de facturación	Información	3	4	3	3	3	Privada	Digital		Gerencia Administrativa / Gerencia Administrativa / Contabilidad /	Contabilidad	Contador	Departamento TI
Formatos gestión documental	Formatos de comunicaciones corporativas y solicitudes	Información	2	2	2	2	2	Privada	Digital		Gerencia Administrativa / Gerencia Administrativa / Gestion Documental /	Gestion Documental	Administrador de Arcivo	Departamento TI
Depto. Financiero Digitalizado	Información digitalizada de departamento financiero	Información	4	3	3	4	4	Confidencial	Digital		Gerencia Administrativa / Gerencia Administrativa / Gestion Documental /	Gestion Documental	Administrador de Arcivo	Departamento TI
Gestión Humana Digitalizado	Documentación digitalizada de Gestión Humana	Información	3	3	4	4	4	Privada	Digital		Gerencia Administrativa / Gerencia Administrativa / Gestion Documental /	Gestion Documental	Administrador de Arcivo	Departamento TI
Carpeta GMA Digitalizado	Carpetas de tipos de siniestros GMA (Internacionales) Digitalizados	Información	4	3	3	4	4	Confidencial	Digital		Gerencia Administrativa / Gerencia Administrativa / Gestion Documental /	Gestion Documental	Administrador de Arcivo	Departamento TI
Carpeta GMC Digitalizado	Carpetas de tipos de siniestros GMC (Nacionales) Digitalizados	Información	4	3	3	4	4	Confidencial	Digital		Gerencia Administrativa / Gerencia Administrativa / Gestion Documental /	Gestion Documental	Administrador de Arcivo	Departamento TI
Carpeta OPA Digitalizado	Carpetas de tipos de siniestros OPA (Ecuador) Digitalizados	Información	3	3	3	3	3	Privada	Digital		Gerencia Administrativa / Gerencia Administrativa / Gestion Documental /	Gestion Documental	Administrador de Arcivo	Departamento TI
Base de datos de prestamos de carpetas físicas	Lista de carpetas prestadas a funcionarios	Información	3	4	3	3	3	Privada	Digital		Gerencia Administrativa / Gestion Documental /	Gestion Documental	Administrador de Arcivo	Departamento TI
Informes de gestión Depto. de Sistemas	Informes de gestión y comunicaciones corporativas de departamento de Sistemas	Información	3	3	3	3	3	Privada	Digital		Gerencia Administrativa / Sistemas/ Informes	Departamento de Sistemas	Líder de Sistemas	Departamento TI
Back Up base de datos	Respaldos de bases de datos de aplicativos	Información	3	5	4	5	5	Confidencial	Digital		Gerencia Administrativa / Sistemas/ Back Up	Departamento de Sistemas	Líder de Sistemas	Departamento TI
Formatos Depto. de Sistemas	Formatos de informes y comunicaciones corporativas	Información	2	2	2	2	2	Privada	Digital		Gerencia Administrativa / Sistemas/ formatos	Departamento de Sistemas	Líder de Sistemas	Departamento TI

Políticas de Seguridad de la información	Documentación de implementación de políticas de seguridad de la información	Información	4	3	3	4	4	Privada	Digital		Gerencia Administrativa / Sistemas / Políticas	Departamento de Sistemas	Lider de Sistemas	Departamento TI
Actas de entregas	Actas de entregas de equipos, Usuarios, cuentas y contraseñas	Información	3	3	2	3	3	Privada	Digital		Gerencia Administrativa / Sistemas/ Actas	Departamento de Sistemas	Lider de Sistemas	Departamento TI
Auditorias Depto. Sistemas	Informes de auditorias	Información	4	2	4	4	4	Privada	Digital		Gerencia Administrativa / Gerencia / Auditorias	Departamento de Sistemas	Lider de Sistemas	Departamento TI
Comunicaciones Depto. Sistemas	Comunicados de fallos y eventualidades en servicios de tecnología	Información	2	1	2	2	2	Privada	Digital		Gerencia Administrativa / Gerencia /	Departamento de Sistemas	Lider de Sistemas	Departamento TI
Diagramas Depto. Sistemas	Diagramas de Procesos	Información	2	2	3	2	2	Privada	Digital		Gerencia Administrativa / Sistemas / Procesos	Departamento de Sistemas	Lider de Sistemas	Departamento TI
Licencias Software	Licencias de servicios de Office 365 y sistemas operativos	Información	4	2	3	4	4	Privada	Digital		Gerencia Administrativa / sistemas / Software	Departamento de Sistemas	Lider de Sistemas	Departamento TI
Roles y procedimientos Depto. Sistemas	Roles y alcance de cargos dentro del departamento de sistemas	Información	2	2	3	3	3	Privada	Digital		Gerencia Administrativa / Gerencia / Procesos	Departamento de Sistemas	Lider de Sistemas	Departamento TI
Metas de facturación	Informe de metas de facturación	Información	3	2	3	3	3	Privada	Digital		Gerencia Administrativa / Gerencia / Administracion	Gerencia Administrativa	Gerente General	Departamento TI
Hojas de vida Funcionarios vinculados	Hojas de vida de funcionarios que trabajan actualmente con Crawford Colombia	Información	4	2	4	3	3	Privada	Digital		Gerencia Administrativa / Recurso Humano	Gerencia Administrativa	Persoal de gestion Humana	Departamento TI
Hojas de vida funcionarios desvinculados	Hojas de vida de funcionarios retirados de Crawford Colombia	Información	4	2	2	2	2	Privada	Digital		Gerencia Administrativa / Recurso Humano	Gerencia Administrativa	Persoal de gestion Humana	Departamento TI
Comunicaciones Gerencia Administrativa	Comunicados y notificaciones a funcionarios	Información	2	3	2	2	2	Privada	Digital		Gerencia Administrativa / Aministracion	Gerencia Administrativa	Persoal de gestion Humana	Departamento TI
Entregas de dotación	Cartas de entregas de dotación	Información	2	2	2	2	2	Privada	Digital		Gerencia Administrativa / Gerencia / Administracion	Gerencia Administrativa	Persoal de gestion Humana	Departamento TI
Perfiles cargo	Documentos de requisitos y requerimientos profesionales para cargos en Crawford Colombia Ltda.	Información	2	3	3	3	3	Privada	Digital		Gerencia Administrativa / Gerencia / Administracion	Gerencia Administrativa	Persoal de gestion Humana	Departamento TI
Documentos de Bancos Aliados	Extractos bancarios	Información	4	4	3	4	4	Confidencial	Digital		Gerencia Administrativa / Gerencia / Administracion	Gerencia Administrativa	Gerente General	Departamento TI
Impuestos	Liquidación de impuestos y normas vigentes	Información	3	4	4	4	4	Confidencial	Digital		Gerencia Administrativa / Gerencia / Administracion	Gerencia Administrativa	Gerente General	Departamento TI
Carpeta de Casos GMC	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMC	Información	4	4	5	5	5	Confidencial	Digital		Operaciones	Operaciones	Director de Operaciones	Departamento TI
Carpeta de Casos GMA	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMA	Información	4	4	5	5	5	Confidencial	Digital		Operaciones	Operaciones	Director de Operaciones	Departamento TI
Informes a Aseguradoras	Informes presentados a clientes con el análisis técnico de Crawford Colombia	Información	4	5	3	4	4	Confidencial	Digital		Operaciones / GMA Operaciones / GMC	Operaciones	Director de Operaciones	Departamento TI
Pólizas	Pólizas suministradas por clientes para el tratamiento del siniestro	Información	3	2	3	3	3	Privada	Digital		Operaciones / GMA Operaciones / GMC	Operaciones	Director de Operaciones	Departamento TI
Fotografías Inspecciones	Fotografías de inspecciones de perdidas y siniestros	Información	4	3	4	4	4	Confidencial	Digital		Operaciones / GMA Operaciones / GMC	Operaciones	Director de Operaciones	Departamento TI
Cuadros de honorarios	Archivos que contienen la descripción del trabajo y las horas empleadas el cual se le presenta a las aseguradoras	Información	4	3	3	3	3	Privada	Digital		Operaciones / GMA Operaciones / GMC	Operaciones	Director de Operaciones	Departamento TI

ANEXO 2 - MATRIZ DE RIESGOS EN LA EMPRESA CRAWFORD COLOMBIA LTDA.

Código Riesgo	Nombre del Activo	Descripción Activo	Tipo Activo	Amenaza	Vulnerabilidades	Redacción del Riesgo	Probabilidad de Ocurrencia		Impacto Credibilidad e Imagen	Impacto Información	Impacto Legal	Impacto Financiero	Impacto Total	Descripción Impacto	Nivel de Riesgo Inherente	
Riesgo_1	Documentos Dirección empresarial	Documentación corporativa de Crawford Colombia	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Documentos Dirección empresarial por Ausencia de identificación y autentificación de emisor y receptor	3	Posible	4	3	2	2	3	Moderado	A	Alto
Riesgo_2	Documentos Dirección empresarial	Documentación corporativa de Crawford Colombia	Información	Corrupción de los datos	Asignación errada de los derechos de acceso	Corrupción de los datos de Documentos Dirección empresarial por Asignación errada de los derechos de acceso	3	Posible	4	4	2	2	3	Moderado	A	Alto
Riesgo_3	Documentos Junta Directiva	Actas de reuniones, Contratos accionistas	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Documentos Junta Directiva por Ausencia de identificación y autentificación de emisor y receptor	3	Posible	2	3	1	1	2	Menor	M	Medio
Riesgo_4	Documentos Junta Directiva	Actas de reuniones, Contratos accionistas	Información	Corrupción de los datos	Asignación errada de los derechos de acceso	Corrupción de los datos de Documentos Junta Directiva por Asignación errada de los derechos de acceso	3	Posible	2	3	1	1	2	Menor	M	Medio
Riesgo_5	Facturas emitidas a clientes internacionales	Facturas pendientes por pagar de clientes internacionales	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Facturas emitidas a clientes internacionales por Asignación errada de los derechos de acceso	3	Posible	4	3	2	2	3	Moderado	A	Alto
Riesgo_6	Facturas emitidas a clientes internacionales	Facturas pendientes por pagar de clientes internacionales	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Facturas emitidas a clientes internacionales por Asignación errada de los derechos de acceso	3	Posible	4	4	2	3	3	Moderado	A	Alto
Riesgo_7	Facturas emitidas a clientes nacionales	Facturas pendientes por pagar de clientes nacionales	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Facturas emitidas a clientes nacionales por Asignación errada de los derechos de acceso	3	Posible	4	3	2	2	3	Moderado	A	Alto
Riesgo_8	Facturas emitidas a clientes nacionales	Facturas pendientes por pagar de clientes nacionales	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Facturas emitidas a clientes nacionales por Asignación errada de los derechos de acceso	3	Posible	4	4	2	3	3	Moderado	A	Alto
Riesgo_9	Informes des gestión de Cartera	Informes de gestión de cobranza y seguimiento de cartera	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Informes des gestión de Cartera por Ausencia de identificación y autentificación de emisor y receptor	3	Posible	3	3	2	3	3	Moderado	A	Alto
Riesgo_10	Informes des gestión de Cartera	Informes de gestión de cobranza y seguimiento de cartera	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Informes des gestión de Cartera por Asignación errada de los derechos de acceso	2	Improbable	2	3	1	1	2	Menor	B	Bajo
Riesgo_11	Certificados de retención proveedores	Certificados de pagos a proveedores	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Certificados de retención proveedores por Ausencia de identificación y autentificación de emisor y receptor	2	Improbable	2	3	1	1	2	Menor	B	Bajo
Riesgo_12	Base de datos proveedores	Lista de proveedores Crawford con información de contactos	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Base de datos proveedores por Asignación errada de los derechos de acceso	1	Raro	1	2	1	1	1	Insignificante	B	Bajo
Riesgo_13	Rut proveedores	Documentación de ubicación y clasificación de proveedores	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Rut proveedores por Asignación errada de los derechos de acceso	2	Improbable	3	2	2	1	2	Menor	B	Bajo
Riesgo_14	Documentos Nomina	Información de pagos a funcionarios vinculados directamente con Crawford Colombia	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Documentos Nomina por Ausencia de identificación y autentificación de emisor y receptor	3	Posible	3	4	2	4	3	Moderado	A	Alto
Riesgo_15	Documentos Nomina	Información de pagos a funcionarios vinculados directamente con Crawford Colombia	Información	Corrupción de los datos	Asignación errada de los derechos de acceso	Corrupción de los datos de Documentos Nomina por Asignación errada de los derechos de acceso	3	Posible	3	4	3	4	4	Mayor	E	Extremo
Riesgo_16	Documentos Nomina	Información de pagos a funcionarios vinculados directamente con Crawford Colombia	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Documentos Nomina por Asignación errada de los derechos de acceso	3	Posible	3	4	3	4	4	Mayor	E	Extremo
Riesgo_17	Pagos Seguridad Social	Certificados de pagos seguridad social	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Pagos Seguridad Social por Asignación errada de los derechos de acceso	2	Improbable	2	3	2	2	2	Menor	B	Bajo
Riesgo_18	Estados Financieros	Informes financieros o estados contables	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Estados Financieros por Ausencia de identificación y autentificación de emisor y receptor	3	Posible	3	3	2	2	3	Moderado	A	Alto
Riesgo_19	Estados Financieros	Informes financieros o estados contables	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Estados Financieros por Asignación errada de los derechos de acceso	2	Improbable	3	3	2	2	3	Moderado	M	Medio
Riesgo_20	Facturas a desarrollar clientes nacionales	Facturas emitidas a aseguradoras o reaseguradoras nacionales	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Facturas a desarrollar clientes nacionales por Ausencia de identificación y autentificación de emisor y receptor	4	Probable	3	3	3	3	3	Moderado	A	Alto
Riesgo_21	Facturas a desarrollar clientes nacionales	Facturas emitidas a aseguradoras o reaseguradoras nacionales	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Facturas a desarrollar clientes nacionales por Asignación errada de los derechos de acceso	4	Probable	4	4	3	4	4	Mayor	E	Extremo
Riesgo_22	facturas desarrolladas clientes internacionales	Facturas emitidas a aseguradoras o reaseguradoras internacionales	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de facturas desarrolladas clientes internacionales por Asignación errada de los derechos de acceso	4	Probable	3	3	3	3	3	Moderado	A	Alto
Riesgo_23	facturas desarrolladas clientes internacionales	Facturas emitidas a aseguradoras o reaseguradoras internacionales	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de facturas desarrolladas clientes internacionales por Asignación errada de los derechos de acceso	4	Probable	4	4	3	4	4	Mayor	E	Extremo
Riesgo_24	Formatos departamento contable	formatos de solicitudes y comunicaciones	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Formatos departamento contable por Asignación errada de los derechos de acceso	2	Improbable	2	3	2	2	2	Menor	B	Bajo
Riesgo_25	Formatos departamento contable	formatos de solicitudes y comunicaciones	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Formatos departamento contable por Asignación errada de los derechos de acceso	2	Improbable	2	3	2	2	2	Menor	B	Bajo
Riesgo_26	Implementación Factura electrónica	Documentación de capacitaciones, reuniones y procesos de facturación electrónica	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Implementación Factura electrónica por Ausencia de identificación y autentificación de emisor y receptor	2	Improbable	2	2	2	3	2	Menor	B	Bajo
Riesgo_27	Implementación Factura electrónica	Documentación de capacitaciones, reuniones y procesos de facturación electrónica	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Implementación Factura electrónica por Asignación errada de los derechos de acceso	2	Improbable	2	2	2	3	2	Menor	B	Bajo
Riesgo_28	Monetizaciones	Certificaciones bancarias de cambios de divisas	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Monetizaciones por Asignación errada de los derechos de acceso	2	Improbable	2	2	2	2	2	Menor	B	Bajo

Riesgo_29	Presupuestos	Presupuestos anuales de Crawford Colombia	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Presupuestos por Asignación errada de los derechos de acceso	2	Improbable	2	2	2	2	2	Menor	B	Bajo
Riesgo_30	Presupuestos	Presupuestos anuales de Crawford Colombia	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Presupuestos por Asignación errada de los derechos de acceso	3	Posible	2	3	2	3	3	Moderado	A	Alto
Riesgo_31	Informes de facturación	Informes mensuales de facturación	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Informes de facturación por Ausencia de identificación y autentificación de emisor y receptor	3	Posible	3	3	2	2	3	Moderado	A	Alto
Riesgo_32	Formatos gestión documental	Formatos de comunicaciones corporativas y solicitudes	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Formatos gestión documental por Asignación errada de los derechos de acceso	2	Improbable	1	2	1	1	1	Insignificante	B	Bajo
Riesgo_33	Formatos gestión documental	Formatos de comunicaciones corporativas y solicitudes	Información	Negación de acciones	Ausencia de identificación y autentificación de emisor y receptor	Negación de acciones de Formatos gestión documental por Ausencia de identificación y autentificación de emisor y receptor	1	Raro	1	3	2	2	2	Menor	B	Bajo
Riesgo_34	Depto. Financiero Digitalizado	Información digitalizada de departamento financiero	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Depto. Financiero Digitalizado por Asignación errada de los derechos de acceso	3	Posible	3	3	2	3	3	Moderado	A	Alto
Riesgo_35	Depto. Financiero Digitalizado	Información digitalizada de departamento financiero	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Depto. Financiero Digitalizado por Asignación errada de los derechos de acceso	3	Posible	3	3	2	3	3	Moderado	A	Alto
Riesgo_36	Gestión Humana Digitalizado	Documentación digitalizada de Gestión Humana	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Gestión Humana Digitalizado por Ausencia de identificación y autentificación de emisor y receptor	3	Posible	2	2	2	1	2	Menor	M	Medio
Riesgo_37	Gestión Humana Digitalizado	Documentación digitalizada de Gestión Humana	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Gestión Humana Digitalizado por Asignación errada de los derechos de acceso	3	Posible	2	3	3	3	3	Moderado	A	Alto
Riesgo_38	Carpeta GMA Digitalizado	Carpetas de tipos de siniestros GMA (Internacionales) Digitalizados	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Carpeta GMA Digitalizado por Asignación errada de los derechos de acceso	3	Posible	4	4	3	3	4	Mayor	E	Extremo
Riesgo_39	Carpeta GMA Digitalizado	Carpetas de tipos de siniestros GMA (Internacionales) Digitalizados	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Carpeta GMA Digitalizado por Asignación errada de los derechos de acceso	3	Posible	1	4	2	2	2	Menor	M	Medio
Riesgo_40	Carpeta GMC Digitalizado	Carpetas de tipos de siniestros GMC (Nacionales) Digitalizados	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Carpeta GMC Digitalizado por Asignación errada de los derechos de acceso	3	Posible	4	4	3	3	4	Mayor	E	Extremo
Riesgo_41	Carpeta GMC Digitalizado	Carpetas de tipos de siniestros GMC (Nacionales) Digitalizados	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Carpeta GMC Digitalizado por Asignación errada de los derechos de acceso	3	Posible	1	4	2	2	2	Menor	M	Medio
Riesgo_42	Carpeta OPA Digitalizado	Carpetas de tipos de siniestros OPA (Ecuador) Digitalizados	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Carpeta OPA Digitalizado por Asignación errada de los derechos de acceso	3	Posible	4	4	3	3	4	Mayor	E	Extremo
Riesgo_43	Carpeta OPA Digitalizado	Carpetas de tipos de siniestros OPA (Ecuador) Digitalizados	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Carpeta OPA Digitalizado por Asignación errada de los derechos de acceso	3	Posible	1	4	2	2	2	Menor	M	Medio
Riesgo_44	Base de datos de prestamos de carpetas físicas	Lista de carpetas prestadas a funcionarios	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Base de datos de prestamos de carpetas físicas por Asignación errada de los derechos de acceso	4	Probable	1	2	1	1	1	Insignificante	M	Medio
Riesgo_45	Informes de gestión Depto. de Sistemas	Informes de gestión y comunicaciones corporativas de departamento de Sistemas	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Informes de gestión Depto. de Sistemas por Asignación errada de los derechos de acceso	3	Posible	2	2	1	1	2	Menor	M	Medio
Riesgo_46	Back Up base de datos	Respaldos de bases de datos de aplicativos	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Back Up base de datos por Asignación errada de los derechos de acceso	4	Probable	4	4	3	4	4	Mayor	E	Extremo
Riesgo_47	Back Up base de datos	Respaldos de bases de datos de aplicativos	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Back Up base de datos por Asignación errada de los derechos de acceso	4	Probable	3	4	2	3	3	Moderado	A	Alto
Riesgo_48	Formatos Depto. de Sistemas	Formatos de informes y comunicaciones corporativas	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Formatos Depto. de Sistemas por Asignación errada de los derechos de acceso	2	Improbable	1	2	1	1	1	Insignificante	B	Bajo
Riesgo_49	Políticas de Seguridad de la información	Documentación de implementación de políticas de seguridad de la información	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Políticas de Seguridad de la información por Asignación errada de los derechos de acceso	3	Posible	2	3	1	1	2	Menor	M	Medio
Riesgo_50	Actas de entregas	Actas de entregas de equipos, Usuarios, cuentas y contraseñas	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Actas de entregas por Asignación errada de los derechos de acceso	3	Posible	2	3	1	1	2	Menor	M	Medio
Riesgo_51	Auditorias Depto. Sistemas	Informes de auditorias	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Auditorias Depto. Sistemas por Asignación errada de los derechos de [illegible]	4	Probable	4	4	3	3	4	Mayor	E	Extremo
Riesgo_52	Comunicaciones Depto. Sistemas	Comunicados de fallos y eventualidades en servicios de tecnología	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Comunicaciones Depto. Sistemas por Asignación errada de los derechos de acceso	2	Improbable	2	2	1	1	2	Menor	B	Bajo
Riesgo_53	Diagramas Depto. Sistemas	Diagramas de Procesos	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de información de Diagramas Depto. Sistemas por Asignación errada de los derechos de [illegible]	3	Posible	2	2	1	1	2	Menor	M	Medio
Riesgo_54	Diagramas Depto. Sistemas	Diagramas de Procesos	Información	Corrupción de los datos	Asignación errada de los derechos de acceso	Corrupción de los datos de Diagramas Depto. Sistemas por Asignación errada de los derechos de acceso	3	Posible	2	3	1	1	2	Menor	M	Medio
Riesgo_55	Licencias Software	Licencias de servicios de Office 365 y sistemas operativos	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Licencias Software por Asignación errada de los derechos de acceso	4	Probable	3	4	5	3	4	Mayor	E	Extremo
Riesgo_56	Roles y procedimientos Depto. Sistemas	Roles y alcance de cargos dentro del departamento de sistemas	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Roles y procedimientos Depto. Sistemas por Asignación errada de los derechos de acceso	3	Posible	2	3	1	1	2	Menor	M	Medio
Riesgo_57	Metas de facturación	Informe de metas de facturación	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Metas de facturación por Asignación errada de los derechos de acceso	3	Posible	2	3	1	1	2	Menor	M	Medio
Riesgo_58	Hojas de vida Funcionarios vinculados	Hojas de vida de funcionarios que trabajan actualmente con Crawford Colombia	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Hojas de vida Funcionarios vinculados por Asignación errada de los derechos de acceso	3	Posible	3	3	4	2	3	Moderado	A	Alto
Riesgo_59	Hojas de vida Funcionarios vinculados	Hojas de vida de funcionarios que trabajan actualmente con Crawford Colombia	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Hojas de vida Funcionarios vinculados por Asignación errada de los derechos de acceso	3	Posible	3	2	2	2	2	Menor	M	Medio
Riesgo_60	Hojas de vida funcionarios desvinculados	Hojas de vida de funcionarios retirados de Crawford Colombia	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Hojas de vida funcionarios desvinculados por Asignación errada de los derechos de acceso	3	Posible	2	3	1	2	2	Menor	M	Medio
Riesgo_61	Comunicaciones Gerencia Administrativa	Comunicados y notificaciones a funcionarios	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Comunicaciones Gerencia Administrativa por Asignación errada de los derechos de acceso	3	Posible	3	2	1	1	2	Menor	M	Medio
Riesgo_62	Entregas de dotación	Cartas de entregas de dotación	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Entregas de dotación por Asignación errada de los derechos de acceso	2	Improbable	2	2	1	1	2	Menor	B	Bajo
Riesgo_63	Perfiles cargo	Documentos de requisitos y requerimientos profesionales para cargos en Crawford Colombia Ltda.	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Perfiles cargo por Asignación errada de los derechos de acceso	3	Posible	3	3	1	2	2	Menor	M	Medio

Riesgo_64	Documentos de Bancos Aliados	Extractos bancarios	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Documentos de Bancos Aliados por Asignación errada de los derechos de acceso	4	Probable	4	4	3	4	4	Mayor	E	Extremo
Riesgo_65	Documentos de Bancos Aliados	Extractos bancarios	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Documentos de Bancos Aliados por Asignación errada de los derechos de acceso	3	Posible	3	4	2	3	3	Moderado	A	Alto
Riesgo_66	Documentos de Bancos Aliados	Extractos bancarios	Información	Corrupción de los datos	Asignación errada de los derechos de acceso	Corrupción de los datos de Documentos de Bancos Aliados por Asignación errada de los derechos de acceso	3	Posible	4	4	3	5	4	Mayor	E	Extremo
Riesgo_67	Impuestos	Liquidación de impuestos y normas vigentes	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Impuestos por Asignación errada de los derechos de acceso	2	Improbable	3	3	2	3	3	Moderado	M	Medio
Riesgo_68	Impuestos	Liquidación de impuestos y normas vigentes	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Impuestos por Asignación errada de los derechos de acceso	3	Posible	2	3	4	4	3	Moderado	A	Alto
Riesgo_69	Carpeta de Casos GMC	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMC	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Carpeta de Casos GMC por Asignación errada de los derechos de acceso	4	Probable	4	4	3	4	4	Mayor	E	Extremo
Riesgo_70	Carpeta de Casos GMC	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMC	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Carpeta de Casos GMC por Asignación errada de los derechos de acceso	4	Probable	5	5	4	5	5	Catastrófico	E	Extremo
Riesgo_71	Carpeta de Casos GMC	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMC	Información	Corrupción de los datos	Asignación errada de los derechos de acceso	Corrupción de los datos de Carpeta de Casos GMC por Asignación errada de los derechos de acceso	4	Probable	4	4	3	3	4	Mayor	E	Extremo
Riesgo_72	Carpeta de Casos GMA	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMA	Información	Divulgación de informacion	Ausencia de identificación y autentificación de emisor y receptor	Divulgación de informacion de Carpeta de Casos GMA por Ausencia de identificación y autentificación de emisor y receptor	4	Probable	2	1	1	2	2	Menor	A	Alto
Riesgo_73	Carpeta de Casos GMA	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMA	Información	Negación de acciones	Asignación errada de los derechos de acceso	Negación de acciones de Carpeta de Casos GMA por Asignación errada de los derechos de acceso	4	Probable	4	4	3	4	4	Mayor	E	Extremo
Riesgo_74	Carpeta de Casos GMA	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMA	Información	Corrupción de los datos	Asignación errada de los derechos de acceso	Corrupción de los datos de Carpeta de Casos GMA por Asignación errada de los derechos de acceso	4	Probable	5	5	4	4	5	Catastrófico	E	Extremo
Riesgo_75	Informes a Aseguradoras	Informes presentados a clientes con el análisis técnico de Crawford Colombia	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Informes a Aseguradoras por Asignación errada de los derechos de acceso	3	Posible	4	4	3	3	4	Mayor	E	Extremo
Riesgo_76	Pólizas	Pólizas suministradas por clientes para el tratamiento del siniestro	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Pólizas por Asignación errada de los derechos de acceso	3	Posible	3	2	1	1	2	Menor	M	Medio
Riesgo_77	Fotografías Inspecciones	Fotografías de inspecciones de perdidas y siniestros	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Fotografías Inspecciones por Asignación errada de los derechos de acceso	3	Posible	4	3	4	4	4	Mayor	E	Extremo
Riesgo_78	Cuadros de honorarios	Archivos que contienen la descripción del trabajo y las horas empleadas el cual se le presenta a las aseguradoras	Información	Divulgación de informacion	Asignación errada de los derechos de acceso	Divulgación de informacion de Cuadros de honorarios por Asignación errada de los derechos de acceso	3	Posible	2	3	2	2	2	Menor	M	Medio
Riesgo_79	Cuadros de honorarios	Archivos que contienen la descripción del trabajo y las horas empleadas el cual se le presenta a las aseguradoras	Información	Corrupción de los datos	Asignación errada de los derechos de acceso	Corrupción de los datos de Cuadros de honorarios por Asignación errada de los derechos de acceso	3	Posible	4	4	2	2	3	Moderado	A	Alto

ANEXO 3 - MATRIZ DE CONTROLES EN LA EMPRESA CRAWFORD COLOMBIA LTDA.

Identificación del Riesgo												Recalificación del Riesgo			
Código Riesgo	Nombre del Activo	Descripción Activo	Tipo Activo	Control	Descripción Control	Control 2	Descripción	Control 3	Descripción	Control 4	Descripción	Probabilidad	Impacto	Nivel de Riesgo Residual	
Riesgo_1	Documentos Dirección empresarial	Documentación corporativa de Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_2	Documentos Dirección empresarial	Documentación corporativa de Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_3	Documentos Junta Directiva	Actas de reuniones, Contratos accionistas	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_4	Documentos Junta Directiva	Actas de reuniones, Contratos accionistas	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_5	Facturas emitidas a clientes internacionales	Facturas pendientes por pagar de clientes internacionales	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_6	Facturas emitidas a clientes internacionales	Facturas pendientes por pagar de clientes internacionales	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_7	Facturas emitidas a clientes nacionales	Facturas pendientes por pagar de clientes nacionales	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_8	Facturas emitidas a clientes nacionales	Facturas pendientes por pagar de clientes nacionales	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_9	Informes des gestión de Cartera	Informes de gestión de cobranza y seguimiento de cartera	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_10	Informes des gestión de Cartera	Informes de gestión de cobranza y seguimiento de cartera	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_11	Certificados de retención proveedores	Certificados de pagos a proveedores	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_12	Base de datos proveedores	Lista de proveedores Crawford con información de contactos	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_13	Rut proveedores	Documentación de ubicación y clasificación de proveedores	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_14	Documentos Nomina	Información de pagos a funcionarios vinculados directamente con Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_15	Documentos Nomina	Información de pagos a funcionarios vinculados directamente con Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Moderado	M	Medio
Riesgo_16	Documentos Nomina	Información de pagos a funcionarios vinculados directamente con Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Moderado	M	Medio
Riesgo_17	Pagos Seguridad Social	Certificados de pagos seguridad social	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de	Raro	Insignificante	B	Bajo
Riesgo_18	Estados Financieros	Informes financieros o estados contables	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_19	Estados Financieros	Informes financieros o estados contables	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_20	Facturas a desarrollar clientes nacionales	Facturas emitidas a aseguradoras o reaseguradoras nacionales	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Menor	B	Bajo
Riesgo_21	Facturas a desarrollar clientes nacionales	Facturas emitidas a aseguradoras o reaseguradoras nacionales	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Moderado	M	Medio
Riesgo_22	facturas desarrolladas clientes internacionales	Facturas emitidas a aseguradoras o reaseguradoras internacionales	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Menor	B	Bajo

Riesgo_23	facturas desarrolladas clientes internacionales	Facturas emitidas a aseguradoras o reaseguradoras internacionales	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Moderado	M	Medio
Riesgo_24	Formatos departamento contable	formatos de solicitudes y comunicaciones	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_25	Formatos departamento contable	formatos de solicitudes y comunicaciones	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_26	Implementación Factura electrónica	Documentación de capacitaciones, reuniones y procesos de facturación electrónica	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_27	Implementación Factura electrónica	Documentación de capacitaciones, reuniones y procesos de facturación electrónica	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_28	Monetizaciones	Certificaciones bancarias de cambios de divisas	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_29	Presupuestos	Presupuestos anuales de Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_30	Presupuestos	Presupuestos anuales de Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_31	Informes de facturación	Informes mensuales de facturación	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_32	Formatos gestión documental	Formatos de comunicaciones corporativas y solicitudes	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_33	Formatos gestión documental	Formatos de comunicaciones corporativas y solicitudes	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_34	Depto. Financiero Digitalizado	Información digitalizada de departamento financiero	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_35	Depto. Financiero Digitalizado	Información digitalizada de departamento financiero	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_36	Gestión Humana Digitalizado	Documentación digitalizada de Gestión Humana	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_37	Gestión Humana Digitalizado	Documentación digitalizada de Gestión Humana	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_38	Carpeta GMA Digitalizado	Carpetas de tipos de siniestros GMA (Internacionales) Digitalizados	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Moderado	M	Medio
Riesgo_39	Carpeta GMA Digitalizado	Carpetas de tipos de siniestros GMA (Internacionales) Digitalizados	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_40	Carpeta GMC Digitalizado	Carpetas de tipos de siniestros GMC (Nacionales) Digitalizados	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Moderado	M	Medio
Riesgo_41	Carpeta GMC Digitalizado	Carpetas de tipos de siniestros GMC (Nacionales) Digitalizados	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_42	Carpeta OPA Digitalizado	Carpetas de tipos de siniestros OPA (Ecuador) Digitalizados	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Moderado	M	Medio
Riesgo_43	Carpeta OPA Digitalizado	Carpetas de tipos de siniestros OPA (Ecuador) Digitalizados	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_44	Base de datos de prestamos de carpetas físicas	Lista de carpetas prestadas a funcionarios	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Insignificante	B	Bajo
Riesgo_45	Informes de gestión Depto. de Sistemas	Informes de gestión y comunicaciones corporativas de departamento de Sistemas	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_46	Back Up base de datos	Respaldos de bases de datos de aplicativos	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Moderado	M	Medio
Riesgo_47	Back Up base de datos	Respaldos de bases de datos de aplicativos	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Menor	B	Bajo

Riesgo_48	Formatos Depto. de Sistemas	Formatos de informes y comunicaciones corporativas	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_49	Políticas de Seguridad de la información	Documentación de implementación de políticas de seguridad de la información	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_50	Actas de entregas	Actas de entregas de equipos, Usuarios, cuentas y contraseñas	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_51	Auditorias Depto. Sistemas	Informes de auditorias	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de	Improbable	Moderado	M	Medio
Riesgo_52	Comunicaciones Depto. Sistemas	Comunicados de fallos y eventualidades en servicios de tecnología	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_53	Diagramas Depto. Sistemas	Diagramas de Procesos	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_54	Diagramas Depto. Sistemas	Diagramas de Procesos	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_55	Licencias Software	Licencias de servicios de Office 365 y sistemas operativos	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Moderado	M	Medio
Riesgo_56	Roles y procedimientos Depto. Sistemas	Roles y alcance de cargos dentro del departamento de sistemas	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_57	Metas de facturación	Informe de metas de facturación	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_58	Hojas de vida Funcionarios vinculados	Hojas de vida de funcionarios que trabajan actualmente con Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_59	Hojas de vida Funcionarios vinculados	Hojas de vida de funcionarios que trabajan actualmente con Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_60	Hojas de vida funcionarios desvinculados	Hojas de vida de funcionarios retirados de Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_61	Comunicaciones Gerencia Administrativa	Comunicados y notificaciones a funcionarios	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_62	Entregas de dotación	Cartas de entregas de dotación	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_63	Perfiles cargo	Documentos de requisitos y requerimientos profesionales para cargos en Crawford Colombia Ltda.	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_64	Documentos de Bancos Aliados	Extractos bancarios	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Moderado	M	Medio
Riesgo_65	Documentos de Bancos Aliados	Extractos bancarios	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_66	Documentos de Bancos Aliados	Extractos bancarios	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Moderado	M	Medio
Riesgo_67	Impuestos	Liquidación de impuestos y normas vigentes	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_68	Impuestos	Liquidación de impuestos y normas vigentes	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo
Riesgo_69	Carpeta de Casos GMC	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMC	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Moderado	M	Medio
Riesgo_70	Carpeta de Casos GMC	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMC	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Mayor	A	Alto
Riesgo_71	Carpeta de Casos GMC	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMC	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Moderado	M	Medio
Riesgo_72	Carpeta de Casos GMA	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMA	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Insignificante	B	Bajo
Riesgo_73	Carpeta de Casos GMA	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia Ltda. por tipo GMA	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Moderado	M	Medio

Riesgo_74	Carpeta de Casos GMA	Carpetas con el seguimiento y procesos de cada siniestro atendido por Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Improbable	Mayor	A	Alto
Riesgo_75	Informes a Aseguradoras	Informes presentados a clientes con el análisis técnico de Crawford Colombia	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Moderado	M	Medio
Riesgo_76	Pólizas	Pólizas suministradas por clientes para el tratamiento del siniestro	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_77	Fotografías Inspecciones	Fotografías de inspecciones de perdidas y siniestros	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Moderado	M	Medio
Riesgo_78	Cuadros de honorarios	Archivos que contienen la descripción del trabajo y las horas empleadas el cual se le presenta a las aseguradoras	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Insignificante	B	Bajo
Riesgo_79	Cuadros de honorarios	Archivos que contienen la descripción del trabajo y las horas empleadas el cual se le presenta a las aseguradoras	Información	Ctrl6	Control de actualizaciones, seguimiento a los accesos y modificaciones de los activos de información.	Ctrl3	Autenticación a nivel de red, mejora la seguridad del servidor de Host de sesión de Escritorio remoto exigiendo que el usuario se autentique antes de crear una sesión.	Ctrl7	Regla del mínimo privilegio, la asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta	Ctrl2	Listas de control de acceso (ACL) extendidas, filtran en las capas 3 y 4, capa de red y capa de transporte, del modelo OSI.	Raro	Menor	B	Bajo